**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC., Plaintiff, v. COMERICA BANK, U.S. BANCORP, AND U.S. BANK NATIONAL ASSOCIATION D/B/A ELAN FINANCIAL SERVICES, Defendants.	CIVIL ACTION NO. 6:21-1052-ADA FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT **JURY TRIAL DEMANDED**

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. ("Textile" or "Plaintiff") files this first amended complaint against Defendants Comerica Bank ("Comerica"), U.S. Bancorp and U.S. Bank National Association d/b/a Elan Financial Services (together, "U.S. Bank") (collectively, "Defendants"), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 6517 Springwood Court, Temple, Texas, 76502.

2. Comerica Bank is a company duly organized and existing under the laws of Texas. Comerica Bank has places of business in Austin, Texas and San Antonio, Texas.

3. Comerica and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country's largest banking and financial service entities, including under the Comerica brand.

4. Comerica and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Comerica and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Comerica and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Comerica and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

8. U.S. Bancorp is a company organized and existing under the laws of Delaware. U.S. Bancorp may be served with process through its registered agent, The Corporation Trust Company, at Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801.

9. U.S. Bank National Association d/b/a Elan Financial Services is a national bank with places of business in Austin, Texas and other locations in Texas. U.S. Bank may be served with process through its registered agent, CT Corporation System, at 4400 Easton Commons Way, Suite 125, Columbus, Ohio 43219.

10. According to U.S. Bancorp, U.S. Bank National Association is "U.S. Bancorp's banking subsidiary" who "is engaged in the general banking business, principally in domestic markets," "provides a wide range of products and services to individuals, businesses,

institutional organizations, governmental entities and other financial institutions" and who has "$465 billion in deposits."[1]

11. The Defendants identified in paragraphs 16-18 above (collectively, "U.S. Bank") and their affiliates lead and are part of an interrelated group of companies which together comprise one of the country's largest banking and financial service entities, including under the U.S. Bank brand, under the Elan Financial Services brand, and under the Elavon brand. Indeed, U.S. Bancorp notes that it has "nearly 70,000 employees and $573 billion in assets" and "serves millions of customers locally, nationally and globally through a diversified mix of businesses: Consumer and Business Banking, Payment Services, Corporate & Commercial Banking and Wealth Management and Investment Services."[2]

12. The U.S. Bank defendants and their affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular. For example, U.S. Bancorp and its subsidiaries are referred to as "the 'Company'" in U.S. Bancorp's annual report, and U.S. Bancorp identified $1.3 billion in "Credit Card Loans" in Texas.[3]

13. The U.S. Bank defendants and their affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

[1] *See* U.S. Bancorp's Form 10-K Annual Report, at 3 (Feb. 22, 2022). https://ir.usbank.com/node/49861/html

[2] *See* U.S. Bancorp's 2021 Annual Report, at 20. https://media.corporate-ir.net/media_files/IROL/usbank/AR2021/pdf/USB_AnnualReport_2021.pdf

[3] *Id* at 22, 32.

14. The U.S. Bank defendants and their affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

15. Thus, the U.S. Bank defendants and their affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

16. The parties to this action are properly joined under 35 U.S.C. § 299 because at least a portion of the right to relief asserted against Defendants jointly and severally arises out of the same series of transactions or occurrences relating to the making and using of the same accused instrumentalities, including authentication systems implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant that are provided, used, and/or made by Defendants. Additionally, questions of fact common to all defendants will arise in this action.

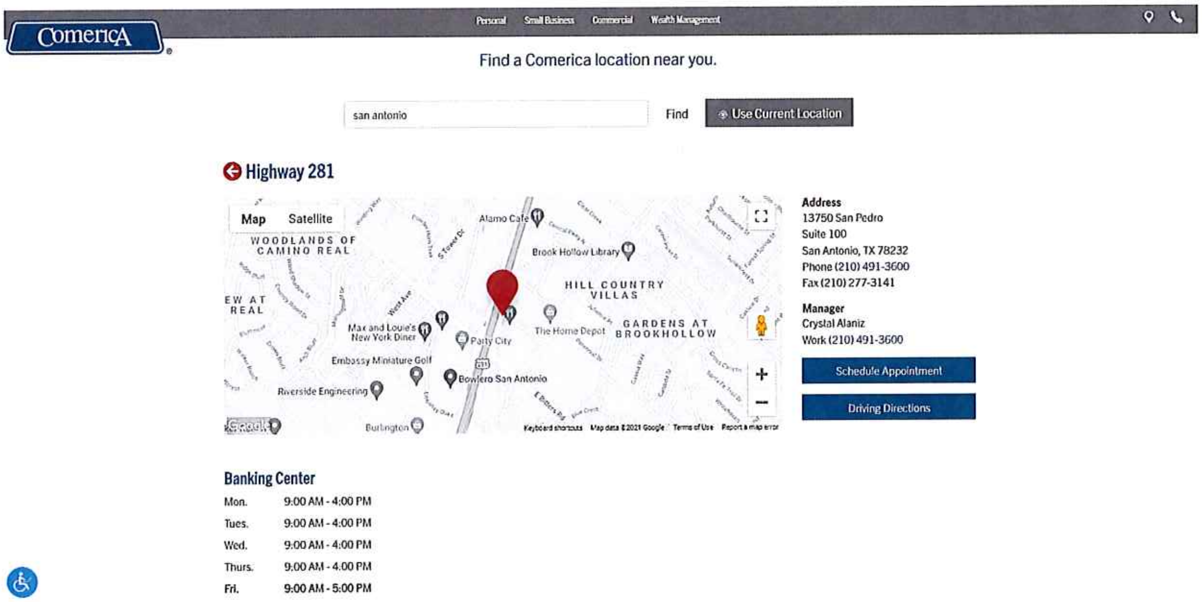
JURISDICTION AND VENUE

17. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

18. This Court has personal jurisdiction over Comerica pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Comerica has done and continues to do business in Texas; and (ii) Comerica has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to

commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

19. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Comerica has committed and continues to commit acts of patent infringement in this district. For example, Comerica cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Comerica induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Comerica has regular and established places of business in this district, including at least at 13750 San Pedro, Suite 100, San Antonio, Texas 78232, at 100 N Santa Rosa St., Suite 110, San Antonio, Texas 78207, and at numerous other locations in San Antonio and Austin:



Find a Comerica location near you.

Highway 281

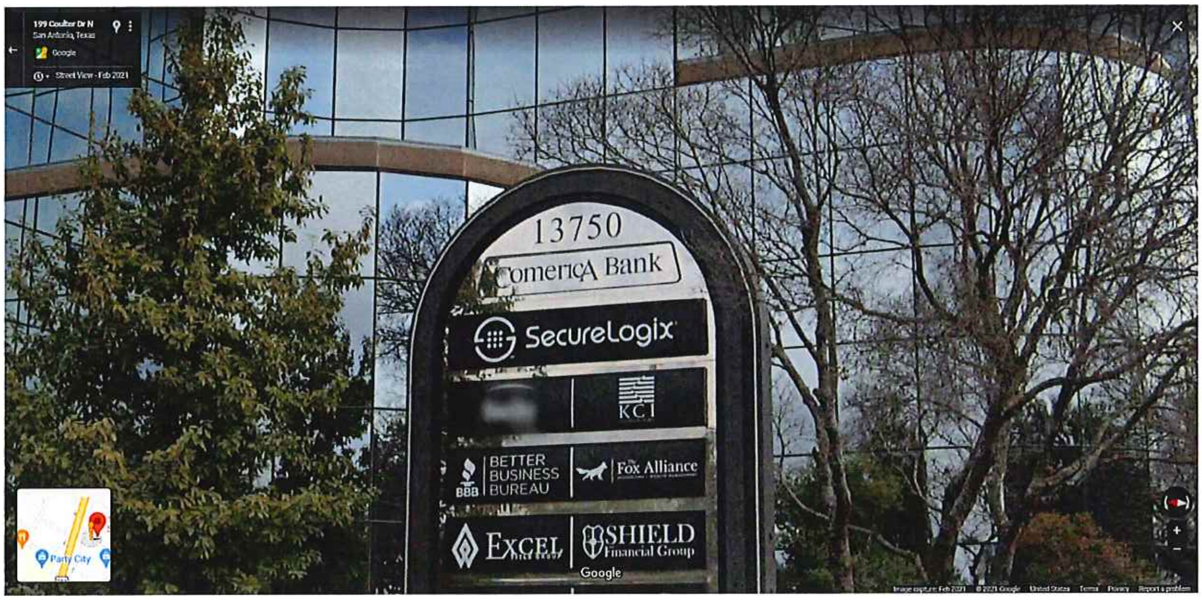
Address
13750 San Pedro
Suite 100
San Antonio, TX 78232
Phone (210) 491-3600
Fax (210) 277-3141

Manager
Crystal Alaniz
Work (210) 491-3600

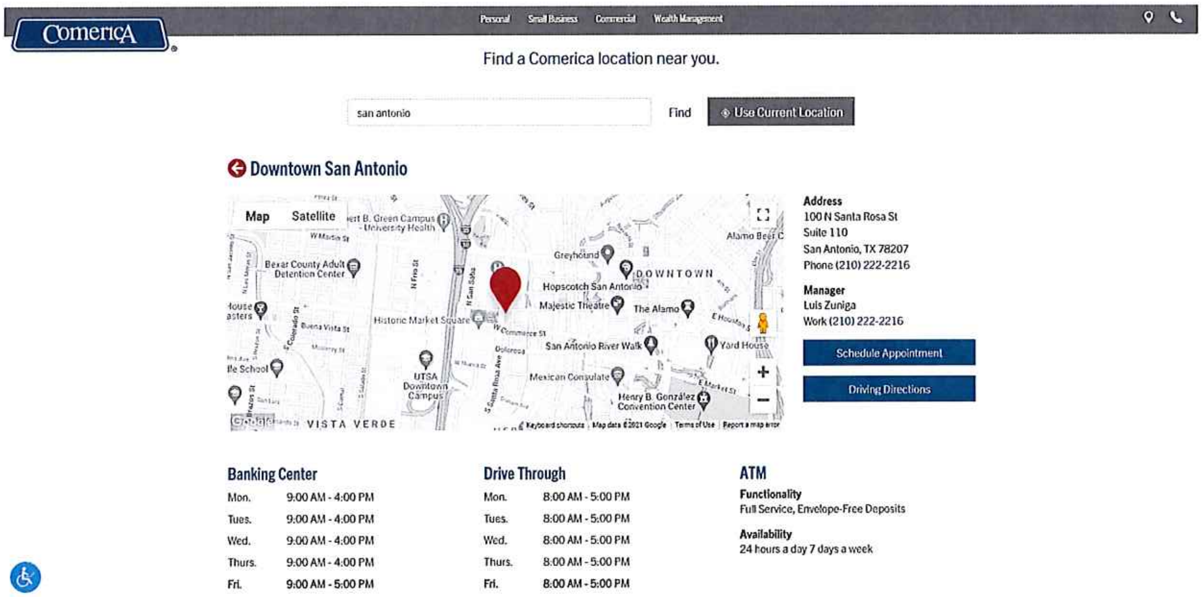
Banking Center

Mon.	9:00 AM - 4:00 PM
Tues.	9:00 AM - 4:00 PM
Wed.	9:00 AM - 4:00 PM
Thurs.	9:00 AM - 4:00 PM
Fri.	9:00 AM - 5:00 PM

(Source: https://locations.comerica.com/location/highway-281?q=san+antonio)



(Source: screenshot from Google Maps Street View)



Find a Comerica location near you.

san antonio | Find | Use Current Location

Downtown San Antonio

Address
100 N Santa Rosa St
Suite 110
San Antonio, TX 78207
Phone (210) 222-2216

Manager
Luis Zuniga
Work (210) 222-2216

Schedule Appointment

Driving Directions

Banking Center

Mon.	9:00 AM - 4:00 PM
Tues.	9:00 AM - 4:00 PM
Wed.	9:00 AM - 4:00 PM
Thurs.	9:00 AM - 4:00 PM
Fri.	9:00 AM - 5:00 PM

Drive Through

Mon.	8:00 AM - 5:00 PM
Tues.	8:00 AM - 5:00 PM
Wed.	8:00 AM - 5:00 PM
Thurs.	8:00 AM - 5:00 PM
Fri.	8:00 AM - 5:00 PM

ATM

Functionality
Full Service, Envelope-Free Deposits

Availability
24 hours a day 7 days a week

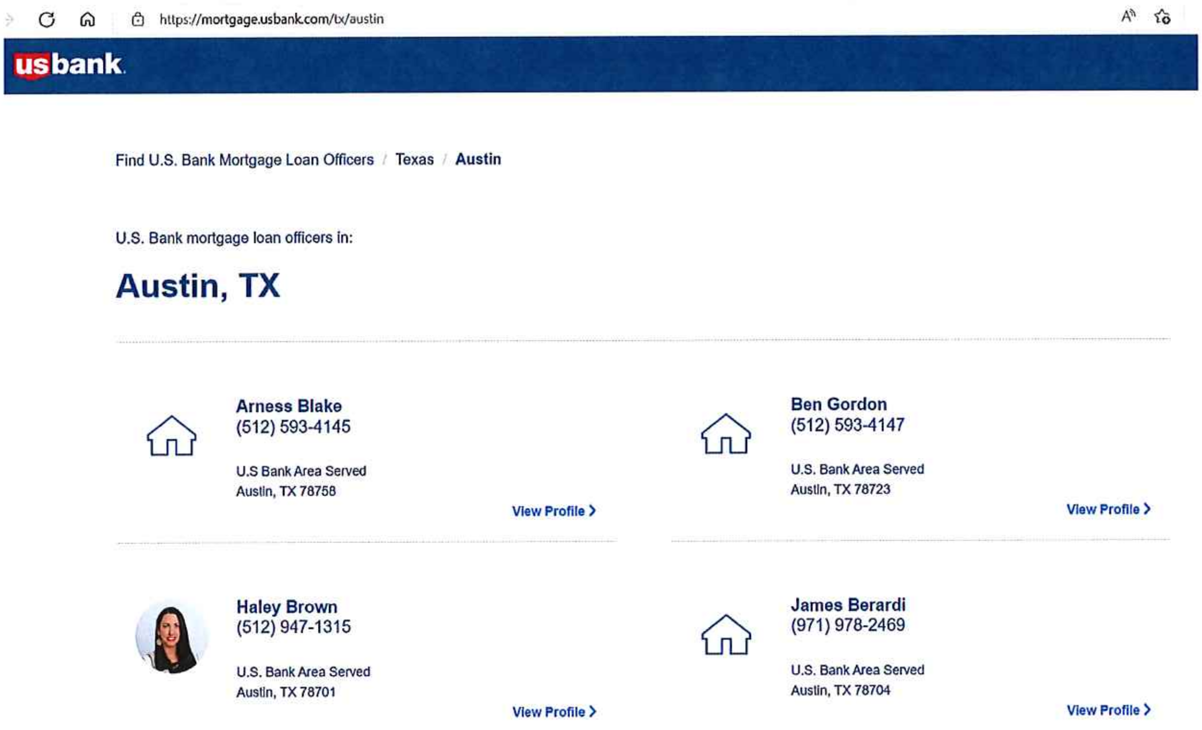
(Source: https://locations.comerica.com/location/downtown-san-antonio?q=san+antonio)

(Source: screenshot from Google Maps Street View)

20. This Court has personal jurisdiction over U.S. Bank pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) U.S. Bank has done and continues to do business in Texas; and (ii) U.S. Bank has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, and via its customers' branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

21. Venue is proper in this district as to U.S. Bank pursuant to 28 U.S.C. § 1400(b). Venue is further proper because U.S. Bank has committed and continues to commit acts of patent infringement in this district. For example, U.S. Bank cardholders, and U.S. Bank's customers' cardholders, are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. U.S. Bank induces others to commit acts of patent infringement

in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. U.S. Bank has regular and established places of business in this district, including at least at in Austin, Texas and Dripping Springs, Texas:


https://mortgage.usbank.com/tx/austin

usbank

Find U.S. Bank Mortgage Loan Officers / Texas / Austin

U.S. Bank mortgage loan officers in:

Austin, TX

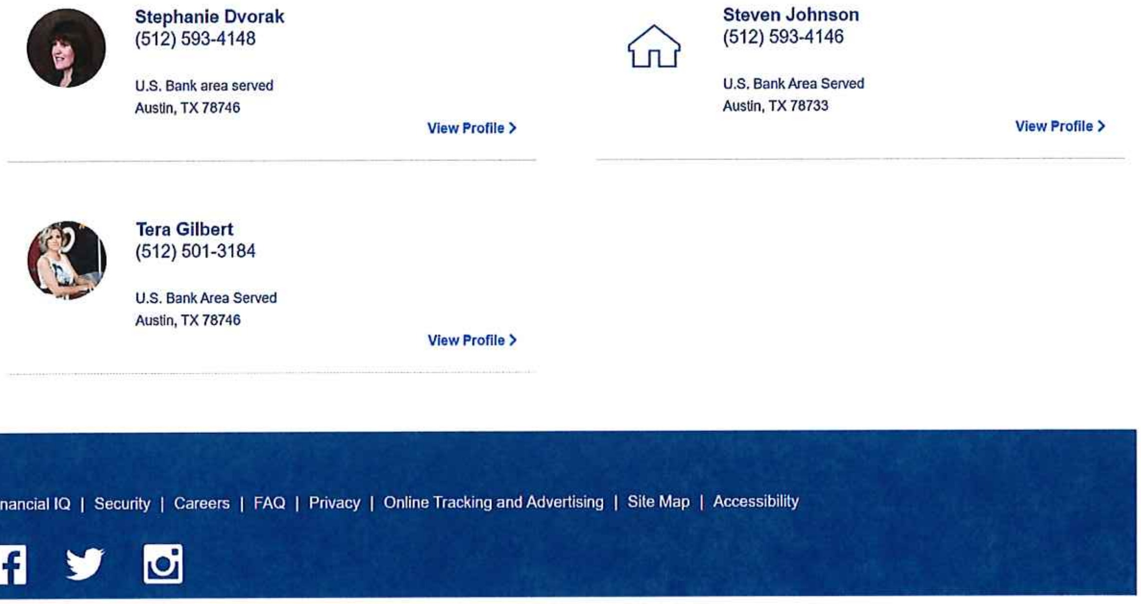
Arness Blake
(512) 593-4145
U.S Bank Area Served
Austin, TX 78758
View Profile >

Ben Gordon
(512) 593-4147
U.S. Bank Area Served
Austin, TX 78723
View Profile >

Haley Brown
(512) 947-1315
U.S. Bank Area Served
Austin, TX 78701
View Profile >

James Berardi
(971) 978-2469
U.S. Bank Area Served
Austin, TX 78704
View Profile >

(Source: https://mortgage.usbank.com/tx/austin)

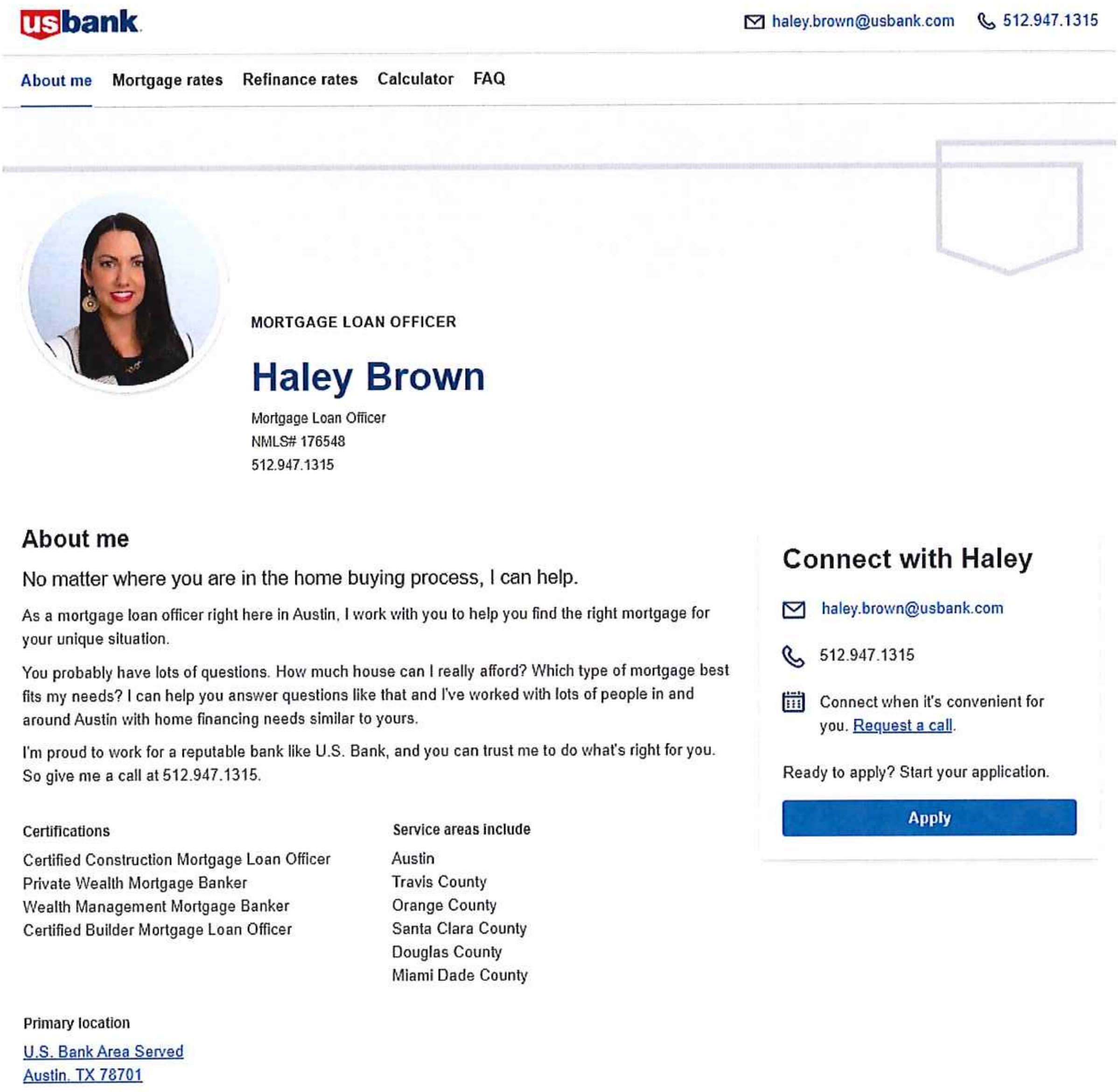

Stephanie Dvorak
(512) 593-4148
U.S. Bank area served
Austin, TX 78746
View Profile >

Steven Johnson
(512) 593-4146
U.S. Bank Area Served
Austin, TX 78733
View Profile >

Tera Gilbert
(512) 501-3184
U.S. Bank Area Served
Austin, TX 78746
View Profile >

Financial IQ | Security | Careers | FAQ | Privacy | Online Tracking and Advertising | Site Map | Accessibility

(Source: https://mortgage.usbank.com/tx/austin)



MORTGAGE LOAN OFFICER

Haley Brown

Mortgage Loan Officer
NMLS# 176548
512.947.1315

About me

No matter where you are in the home buying process, I can help.

As a mortgage loan officer right here in Austin, I work with you to help you find the right mortgage for your unique situation.

You probably have lots of questions. How much house can I really afford? Which type of mortgage best fits my needs? I can help you answer questions like that and I've worked with lots of people in and around Austin with home financing needs similar to yours.

I'm proud to work for a reputable bank like U.S. Bank, and you can trust me to do what's right for you. So give me a call at 512.947.1315.

Certifications

Certified Construction Mortgage Loan Officer
Private Wealth Mortgage Banker
Wealth Management Mortgage Banker
Certified Builder Mortgage Loan Officer

Service areas include

Austin
Travis County
Orange County
Santa Clara County
Douglas County
Miami Dade County

Primary location

U.S. Bank Area Served
Austin, TX 78701

Connect with Haley

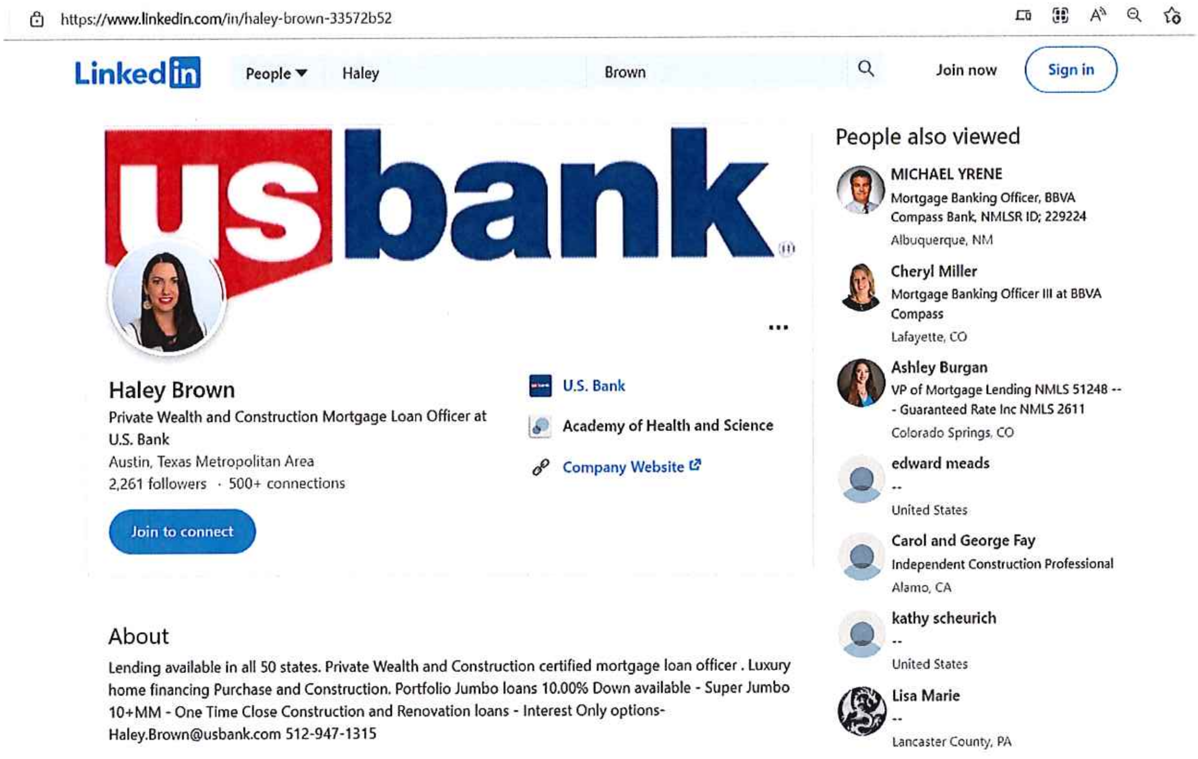
✉ haley.brown@usbank.com

☎ 512.947.1315

Connect when it's convenient for you. Request a call.

Ready to apply? Start your application.

(Source: https://mortgage.usbank.com/tx-austin-haley-brown)



Haley Brown

Private Wealth and Construction Mortgage Loan Officer at U.S. Bank

Austin, Texas Metropolitan Area

2,261 followers · 500+ connections

U.S. Bank

Academy of Health and Science

Company Website

About

Lending available in all 50 states. Private Wealth and Construction certified mortgage loan officer . Luxury home financing Purchase and Construction. Portfolio Jumbo loans 10.00% Down available - Super Jumbo 10+MM - One Time Close Construction and Renovation loans - Interest Only options- Haley.Brown@usbank.com 512-947-1315

People also viewed

MICHAEL YRENE
Mortgage Banking Officer, BBVA Compass Bank, NMLSR ID; 229224
Albuquerque, NM

Cheryl Miller
Mortgage Banking Officer III at BBVA Compass
Lafayette, CO

Ashley Burgan
VP of Mortgage Lending NMLS 51248 -- - Guaranteed Rate Inc NMLS 2611
Colorado Springs, CO

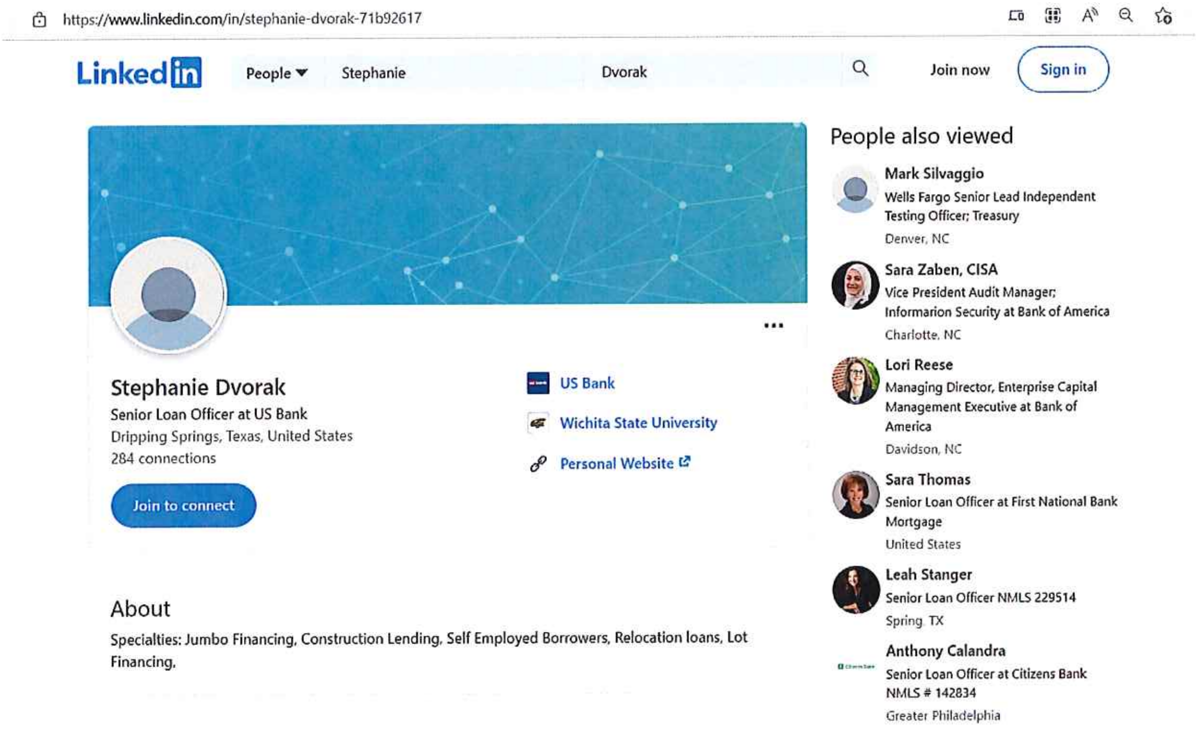
edward meads
--
United States

Carol and George Fay
Independent Construction Professional
Alamo, CA

kathy scheurich
--
United States

Lisa Marie
--
Lancaster County, PA

(Source: https://www.linkedin.com/in/haley-brown-33572b52)



Stephanie Dvorak

Senior Loan Officer at US Bank

Dripping Springs, Texas, United States

284 connections

US Bank

Wichita State University

Personal Website

About

Specialties: Jumbo Financing, Construction Lending, Self Employed Borrowers, Relocation loans, Lot Financing.

People also viewed

Mark Silvaggio
Wells Fargo Senior Lead Independent Testing Officer; Treasury
Denver, NC

Sara Zaben, CISA
Vice President Audit Manager; Information Security at Bank of America
Charlotte, NC

Lori Reese
Managing Director, Enterprise Capital Management Executive at Bank of America
Davidson, NC

Sara Thomas
Senior Loan Officer at First National Bank Mortgage
United States

Leah Stanger
Senior Loan Officer NMLS 229514
Spring, TX

Anthony Calandra
Senior Loan Officer at Citizens Bank NMLS # 142834
Greater Philadelphia

(Source: https://www.linkedin.com/in/stephanie-dvorak-71b92617)

BACKGROUND

22. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

23. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

24. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

25. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the "Asserted Patents"), teach systems, including payment processing systems, for securely and effectively approving and processing specific

credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

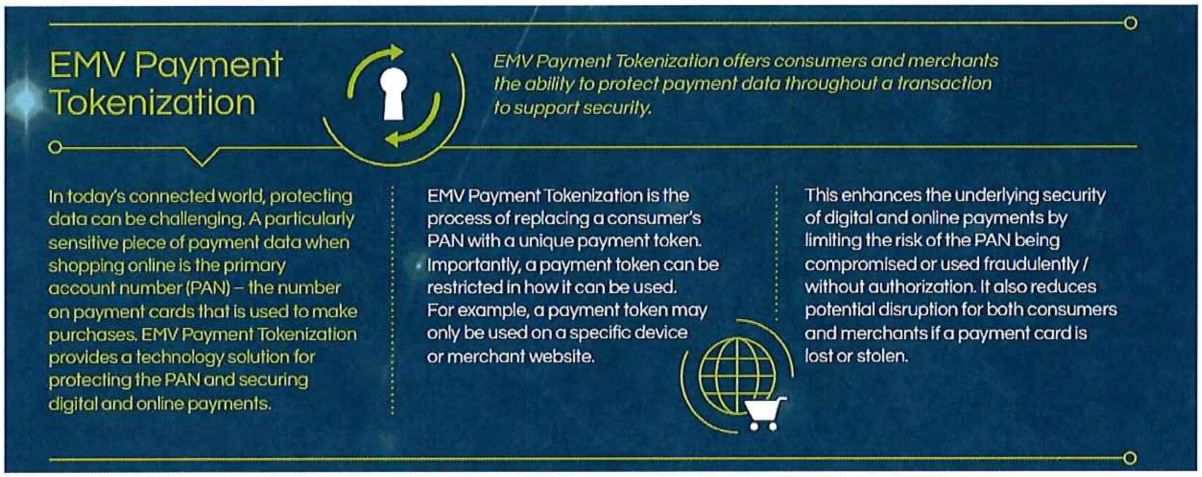
26. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall's, was hit with a cyber attack that resulted in the theft of credit cards leading to over $100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

27. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as "a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment" and as "enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs." (Source: https://www.emvco.com/emv-technologies/payment-tokenisation/).

28. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a

number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

29. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents "provides a technology solution for protecting the PAN and securing digital and online payments":



EMV Payment Tokenization

EMV Payment Tokenization offers consumers and merchants the ability to protect payment data throughout a transaction to support security.

In today's connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases. EMV Payment Tokenization provides a technology solution for protecting the PAN and securing digital and online payments.

EMV Payment Tokenization is the process of replacing a consumer's PAN with a unique payment token. Importantly, a payment token can be restricted in how it can be used. For example, a payment token may only be used on a specific device or merchant website.

This enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization. It also reduces potential disruption for both consumers and merchants if a payment card is lost or stolen.

(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

30. That same EMVCo document notes that "In today's connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases" and that EMVCo's payment tokenization "enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization." The document also states that the "Payment Tokenisation Specification provides an interoperable Technical Framework." (Source: https://www.emvco.com/wp-

content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

31. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office ("PTO"). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the "key string" as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

COUNT I

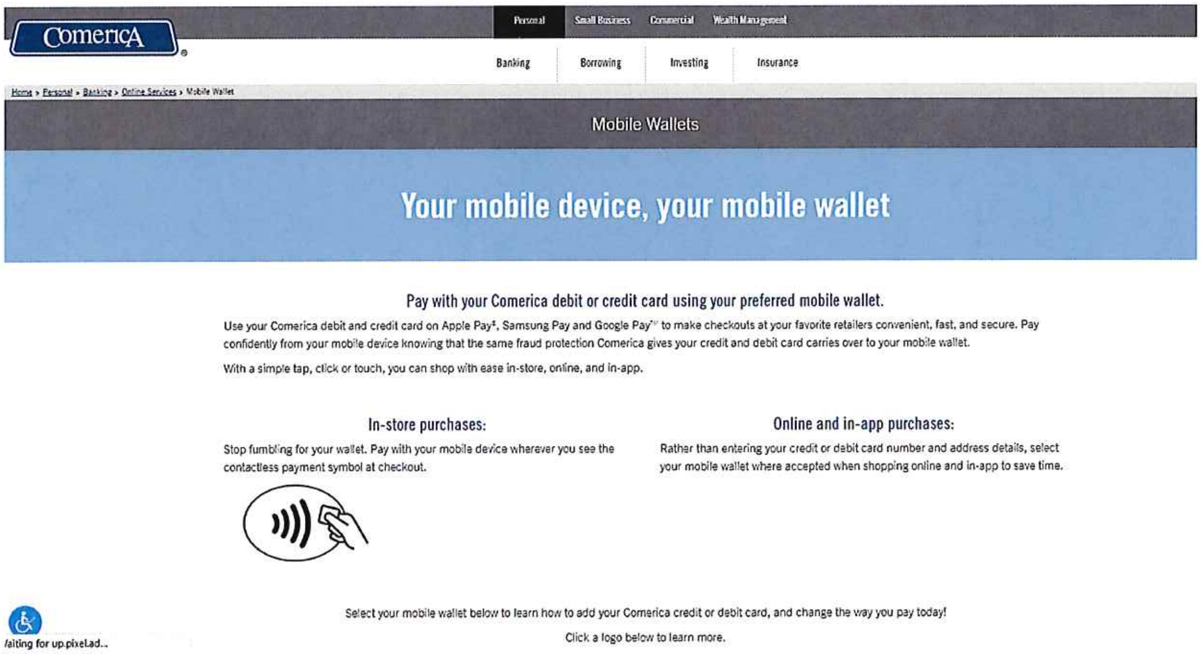
INFRINGEMENT OF U.S. PATENT NO. 8,505,079

32. On August 6, 2013, United States Patent No. 8,505,079 ("the 079 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Related Method."

33. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

34. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard and Visa Credit Card, that are used with an authentication system that authenticates the identity of a card holder in a request to pay a merchant for a transaction (the "Accused Instrumentality"). U.S. Bank offers debit and/or credit cards, such as the U.S. Bank Visa Debit Card and the U.S. Bank Visa Platinum Card, that are also used with the Accused Instrumentality card authentication system. U.S. Bank also provides services to other banks (including, but not limited to, Broadway National Bank, Comerica, Independent Bank, Southside Bank, and Texas

Capital Bank) for the purposes of using the Accused Instrumentality card authentication system. The Accused Instrumentality card authentication systems that are used, made, and sold by Comerica and U.S. Bank are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Mobile Wallets

Your mobile device, your mobile wallet

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay‡, Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

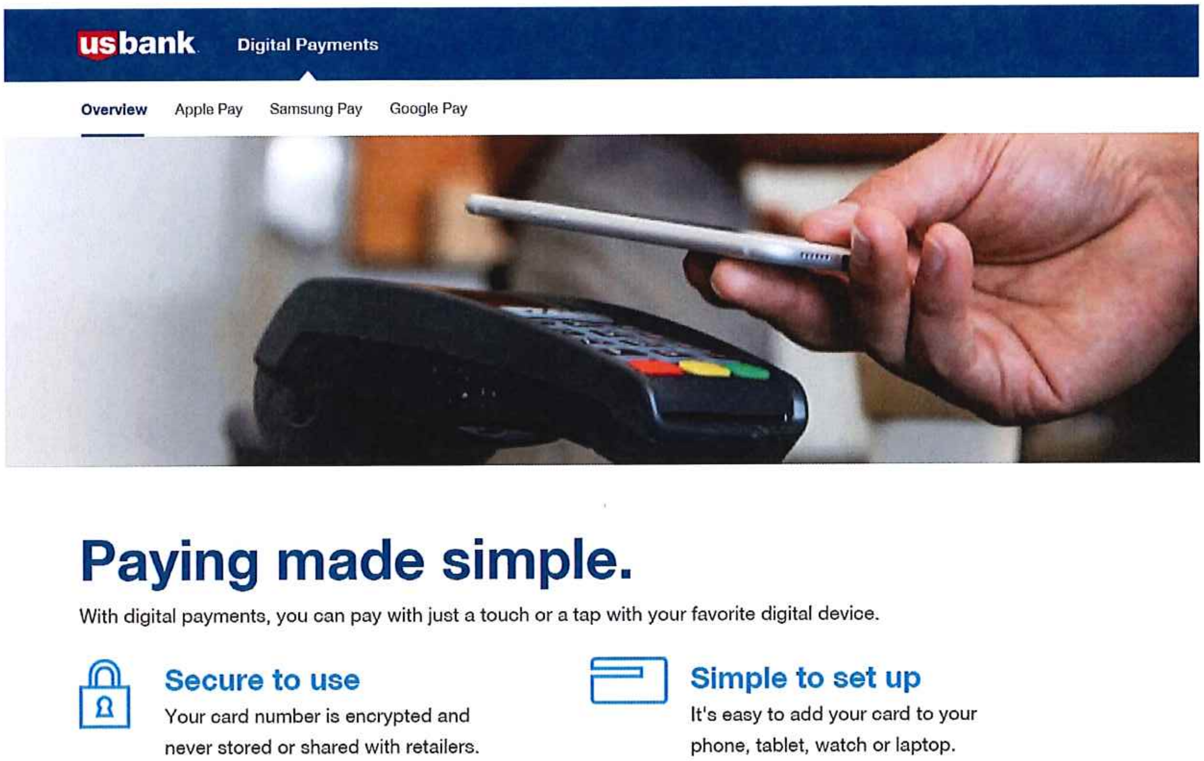
Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html)



Paying made simple.

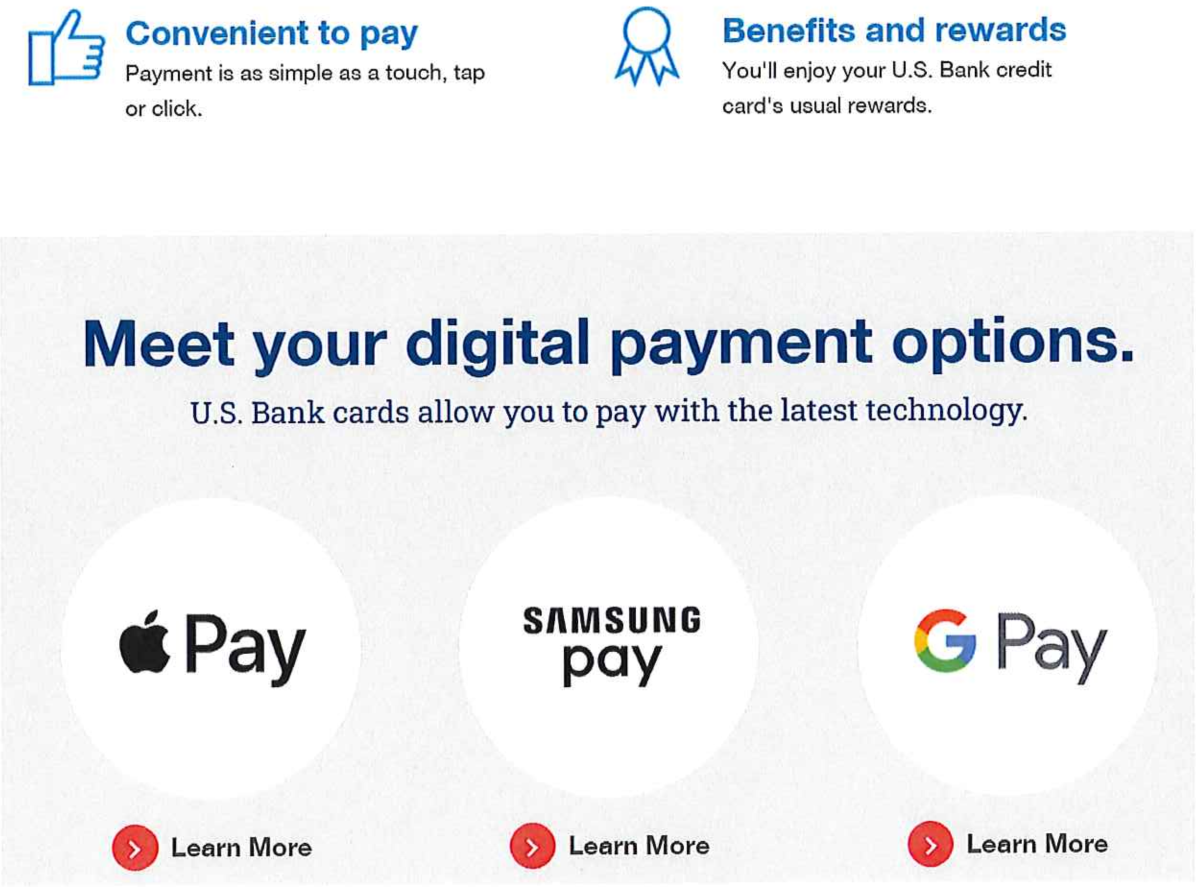
With digital payments, you can pay with just a touch or a tap with your favorite digital device.

Secure to use

Your card number is encrypted and never stored or shared with retailers.

Simple to set up

It's easy to add your card to your phone, tablet, watch or laptop.



Convenient to pay

Payment is as simple as a touch, tap or click.

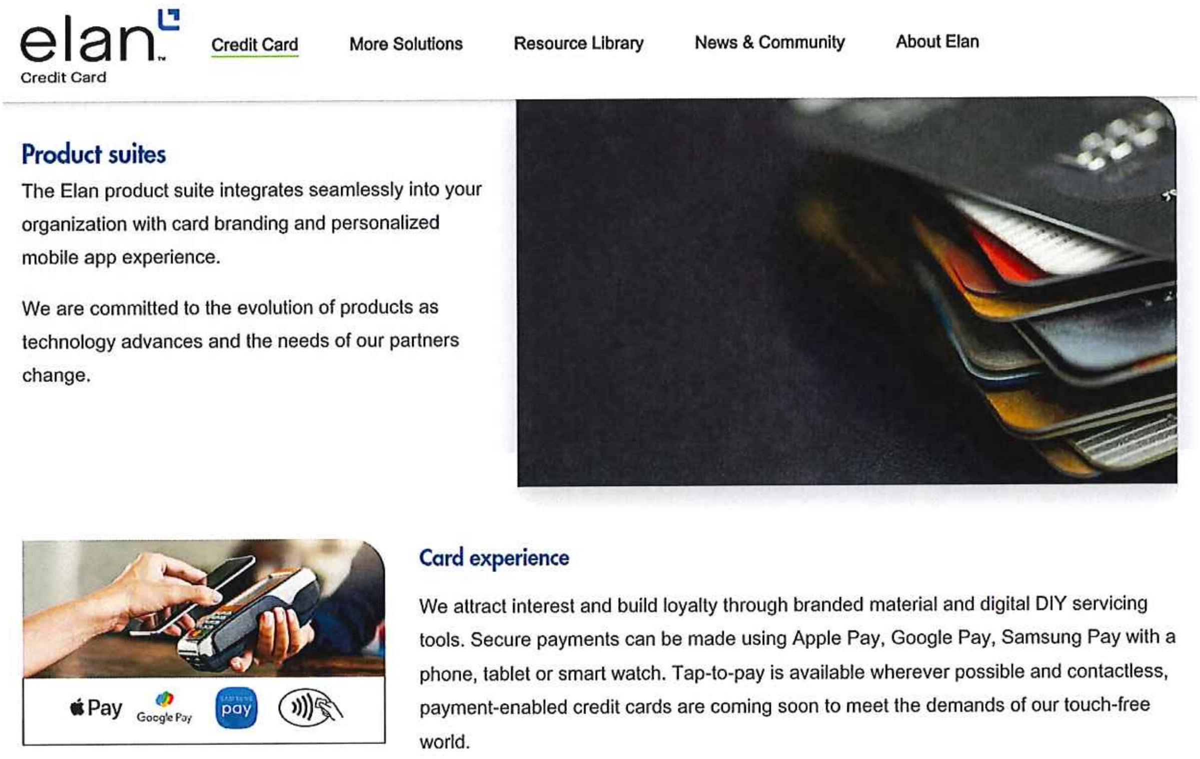
Benefits and rewards

You'll enjoy your U.S. Bank credit card's usual rewards.

Meet your digital payment options.

U.S. Bank cards allow you to pay with the latest technology.

(Source: https://www.usbankgomobile.com/wallet/#/home)



Product suites

The Elan product suite integrates seamlessly into your organization with card branding and personalized mobile app experience.

We are committed to the evolution of products as technology advances and the needs of our partners change.

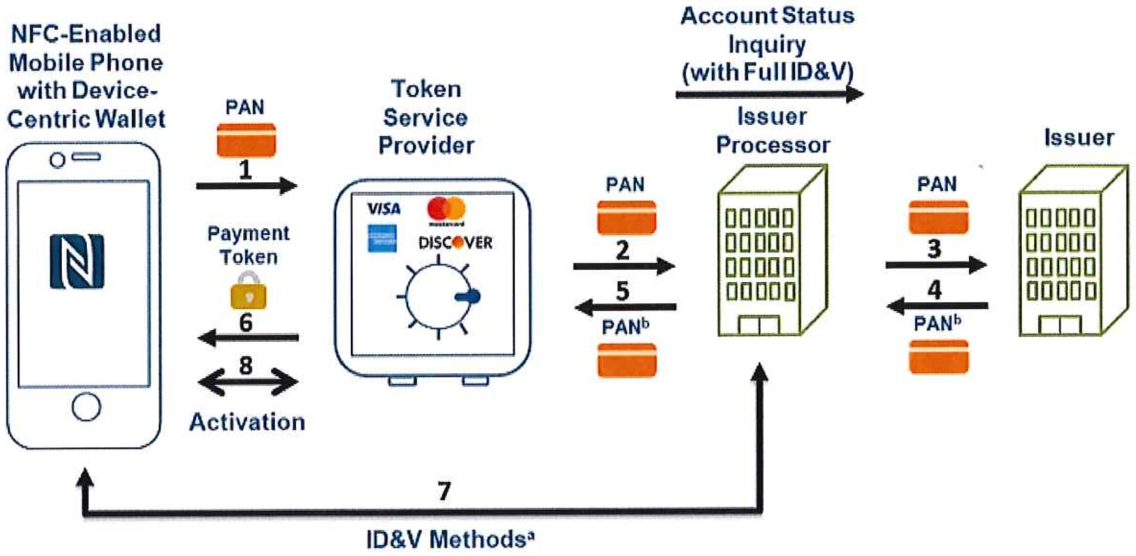
Card experience

We attract interest and build loyalty through branded material and digital DIY servicing tools. Secure payments can be made using Apple Pay, Google Pay, Samsung Pay with a phone, tablet or smart watch. Tap-to-pay is available wherever possible and contactless, payment-enabled credit cards are coming soon to meet the demands of our touch-free world.

(Source: https://www.elanfinancialservices.com/credit-card/what-we-offer/product-suites.html)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.

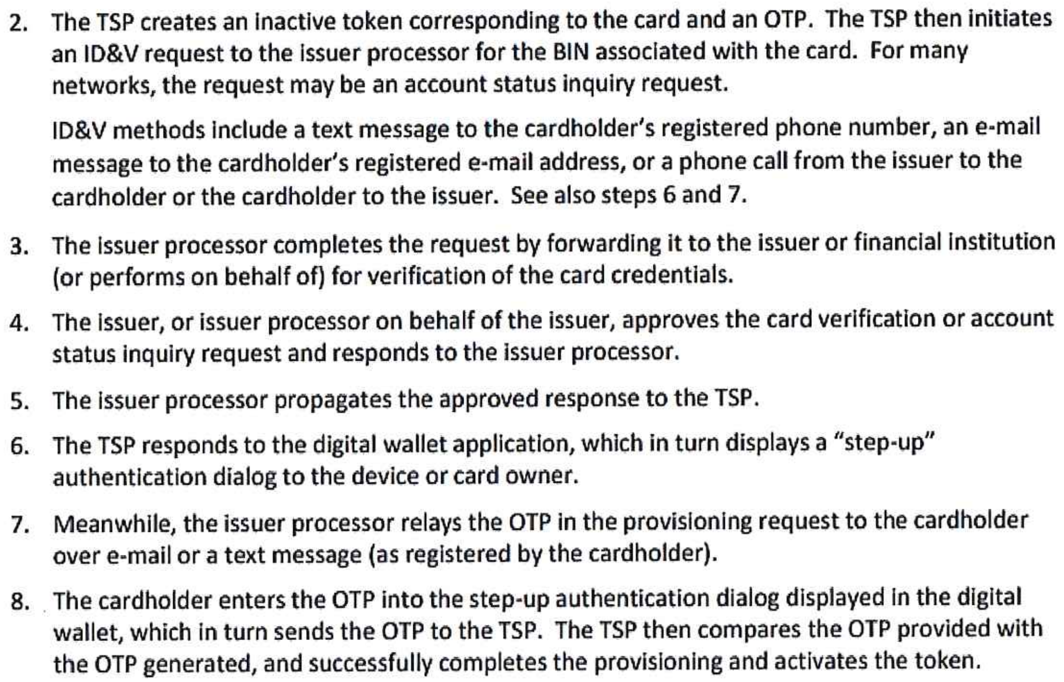


[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.



2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

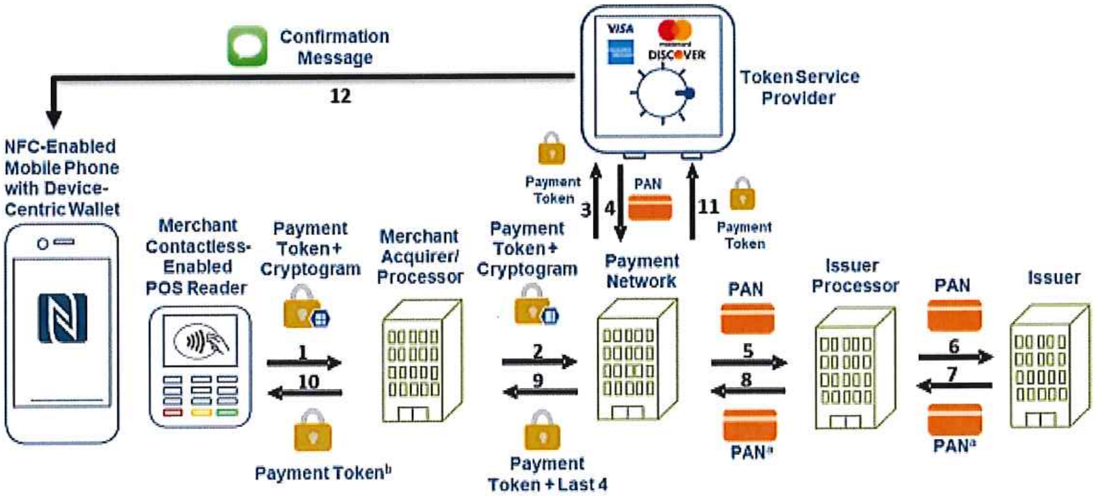
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

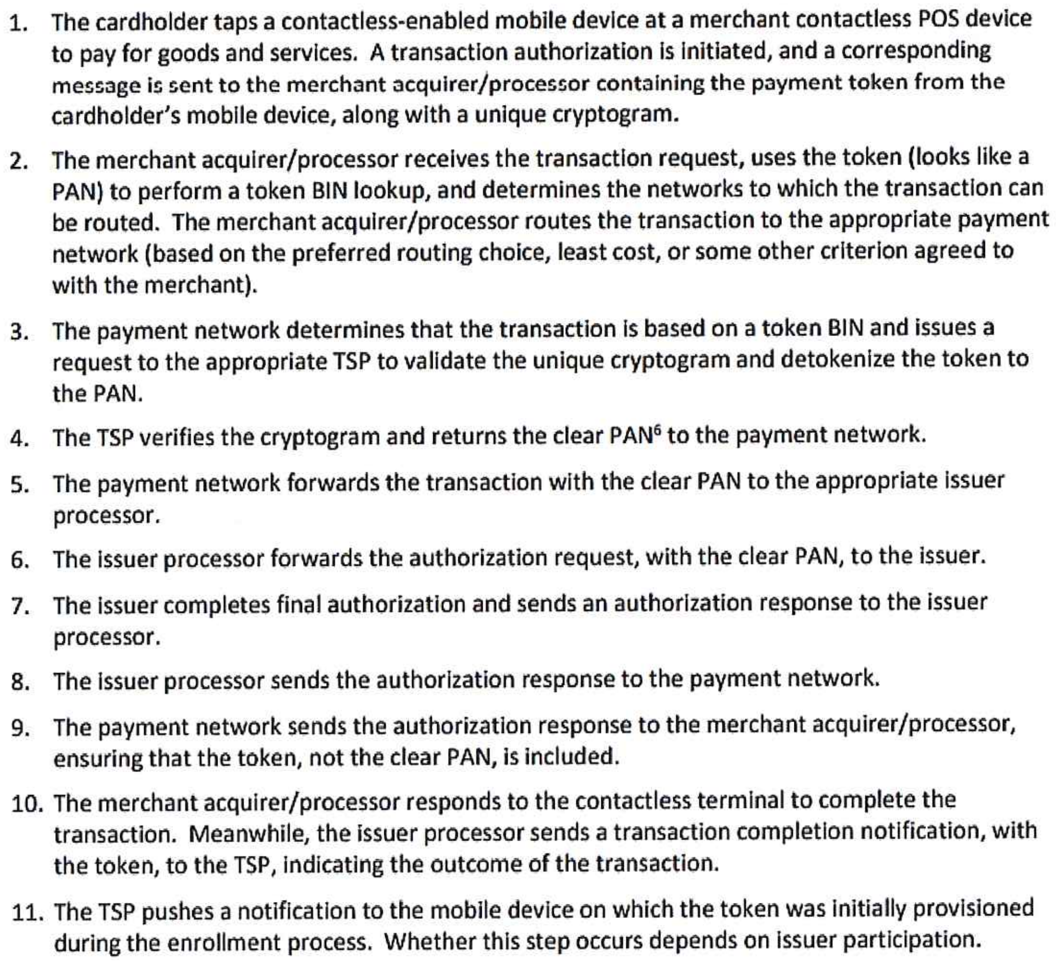
Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:



1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

35. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, an account holder of Defendant (or an account holder of a customer bank of Defendant) requests Defendant (or its customer bank) to provision a specific debit and/or credit card of Defendant (or its customer bank) for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her smartphone when

near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

36. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by a card holder of a debit and/or credit card of Defendant (or its customer bank) for provisioning a specific debit and/or credit card of a cardholder customer of Defendant (or its customer bank) for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by a cardholder customer of Defendant (or its customer bank) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of a cardholder customer of Defendant (or its customer bank). This messaging gateway is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

37. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer

readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

38. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

39. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

40. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

41. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

42. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

43. Defendants have directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

44. In the pre-suit period, Comerica has indirectly infringed (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Comerica will continue to

do so unless enjoined by this Court. Comerica's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Comerica knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

45. In the post-suit period, Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Defendants will continue to do so unless enjoined by this Court. Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the

induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

46. In the pre-suit period, Comerica has made, used, made available for another's use, sold or offered to sell, the Accused Instrumentality, and/or have induced others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

47. In the post-suit period, Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

48. Defendants have committed these acts of infringement without license or authorization.

49. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

50. As a direct and proximate result of Defendants' infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

51. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause

immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

52. Comerica has had actual knowledge of the 079 Patent at least as of October 18, 2013, when Textile sent a letter to Ralph W. Babb, Jr., then Chief Executive Officer of Comerica Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

53. Comerica has had actual knowledge of the 079 Patent at least as of November 10, 2014, when Textile sent a letter to Ralph W. Babb, Jr., then Chief Executive Officer of Comerica Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

54. Defendants have had actual knowledge of the 079 Patent at least as of the date when they were notified of the filing of this action. By the time of trial, Defendants will have known and intended (since receiving such notice) that their continued actions would infringe and actively induce the infringement of one or more claims of the 079 Patent.

55. In the pre-suit period, Comerica has indirectly and willfully infringed the 079 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

56. In the post-suit period, Defendants have also indirectly and willfully infringed, and continue to indirectly and willfully infringe, the 079 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

57. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

58. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

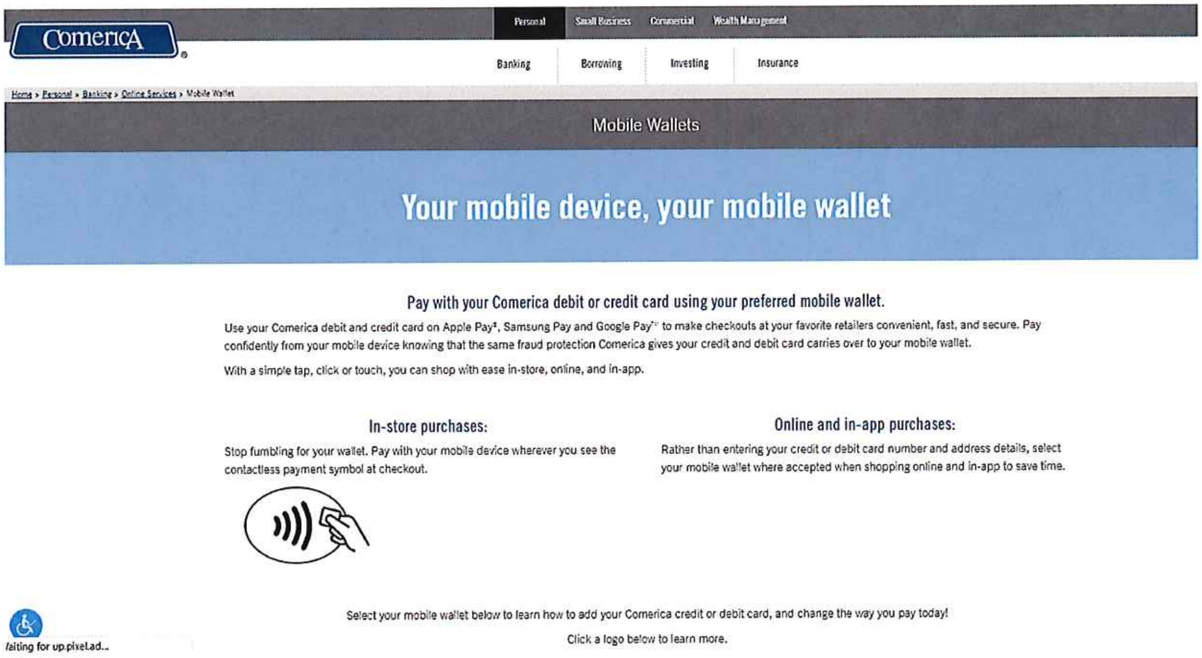
INFRINGEMENT OF U.S. PATENT NO. 8,533,802

59. On September 10, 2013, United States Patent No. 8,533,802 ("the 802 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Related Method."

60. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

61. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard and Visa Credit Card, that are used with an authentication system that authenticates the identity of a card holder in a request to pay a merchant for a transaction (the "Accused Instrumentality"). U.S. Bank offers debit and/or credit cards, such as the U.S. Bank Visa Debit Card and the U.S. Bank Visa Platinum Card, that are also used with the Accused Instrumentality card authentication system. U.S. Bank also provides services to other banks (including, but not limited to, Broadway National Bank, Comerica, Independent Bank, Southside Bank, and Texas Capital Bank) for the purposes of using the Accused Instrumentality card authentication system. The Accused Instrumentality card authentication systems that are used, made, and sold by

Comerica and U.S. Bank are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Mobile Wallets

Your mobile device, your mobile wallet

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay², Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

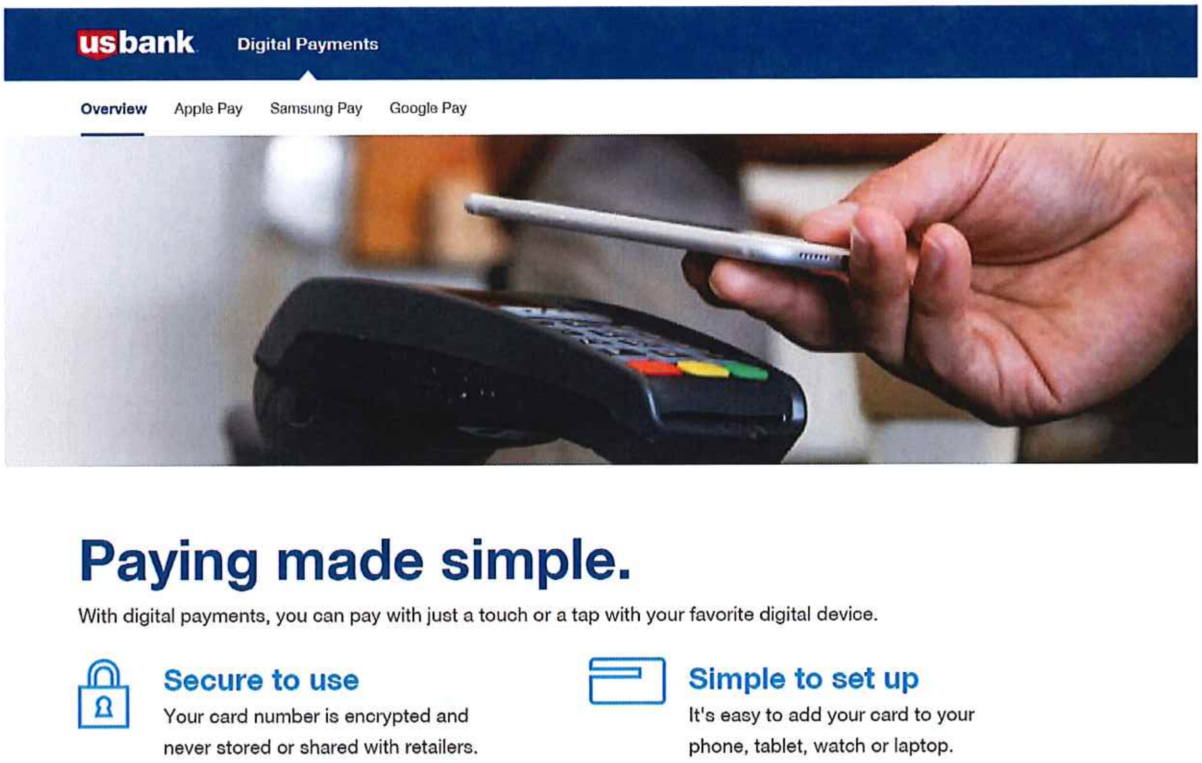
Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html)



Paying made simple.

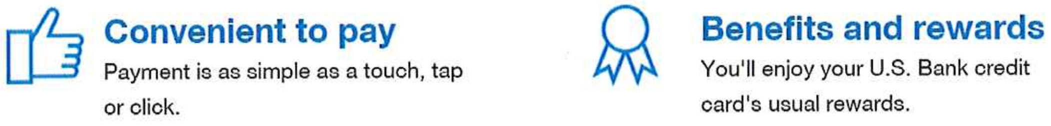
With digital payments, you can pay with just a touch or a tap with your favorite digital device.

Secure to use

Your card number is encrypted and never stored or shared with retailers.

Simple to set up

It's easy to add your card to your phone, tablet, watch or laptop.

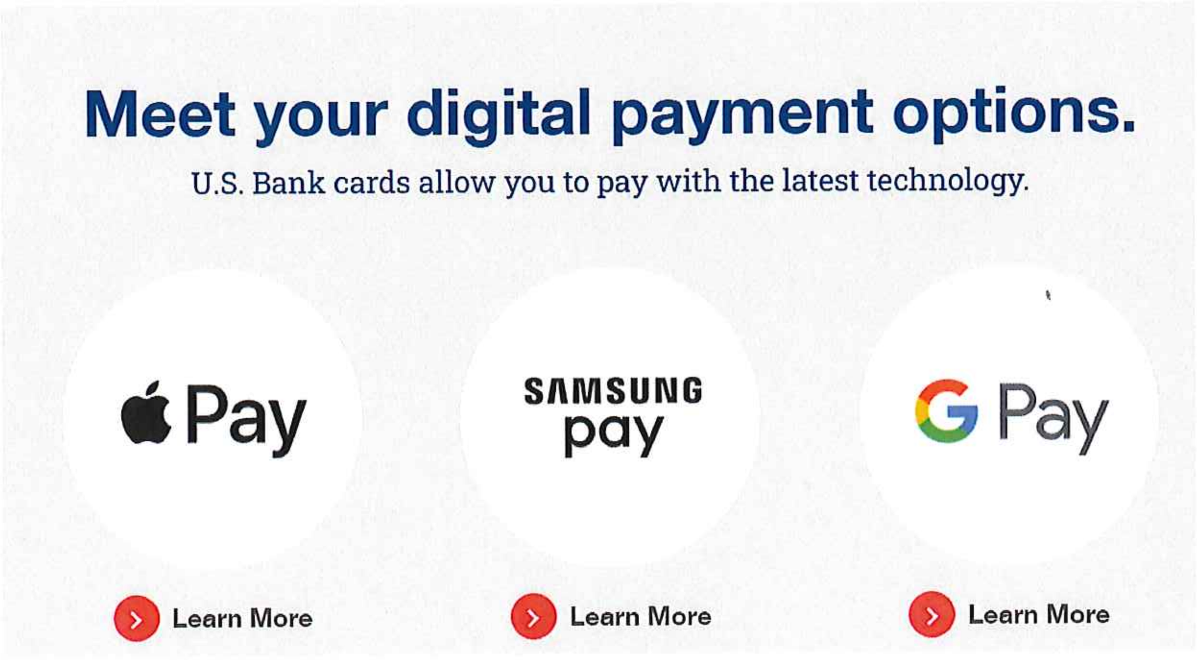


Convenient to pay

Payment is as simple as a touch, tap or click.

Benefits and rewards

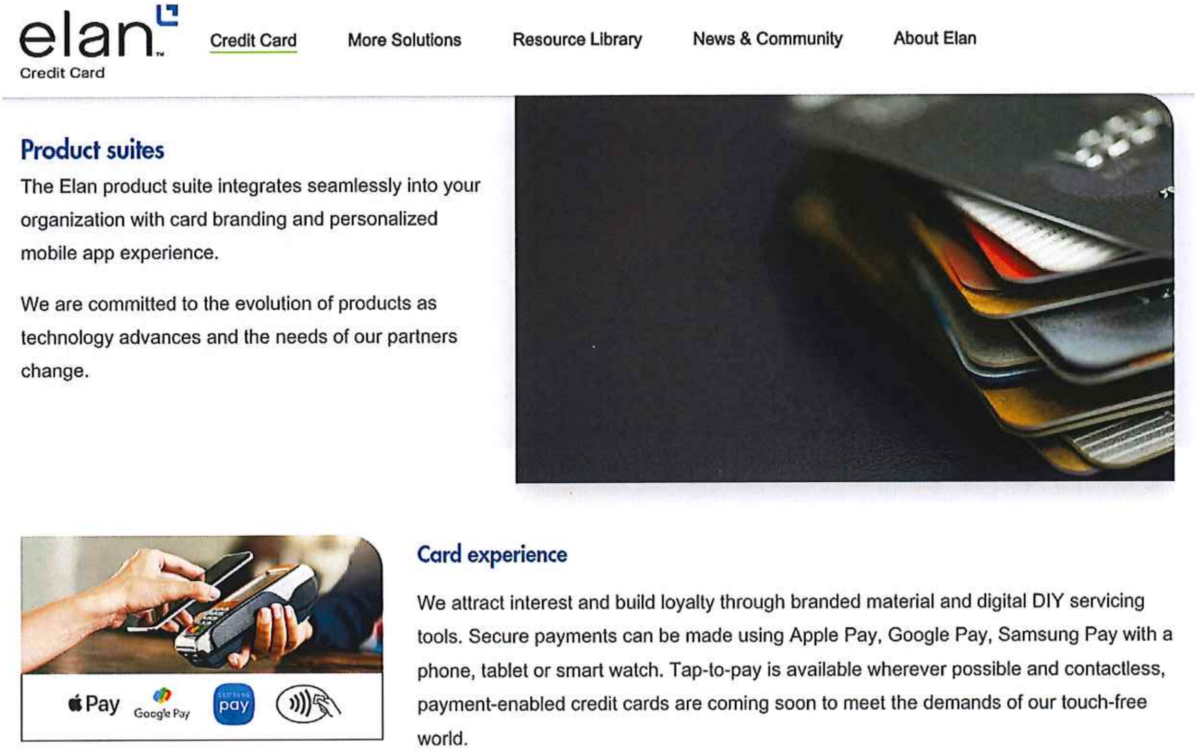
You'll enjoy your U.S. Bank credit card's usual rewards.



Meet your digital payment options.

U.S. Bank cards allow you to pay with the latest technology.

(Source: https://www.usbankgomobile.com/wallet/#/home)



Product suites

The Elan product suite integrates seamlessly into your organization with card branding and personalized mobile app experience.

We are committed to the evolution of products as technology advances and the needs of our partners change.

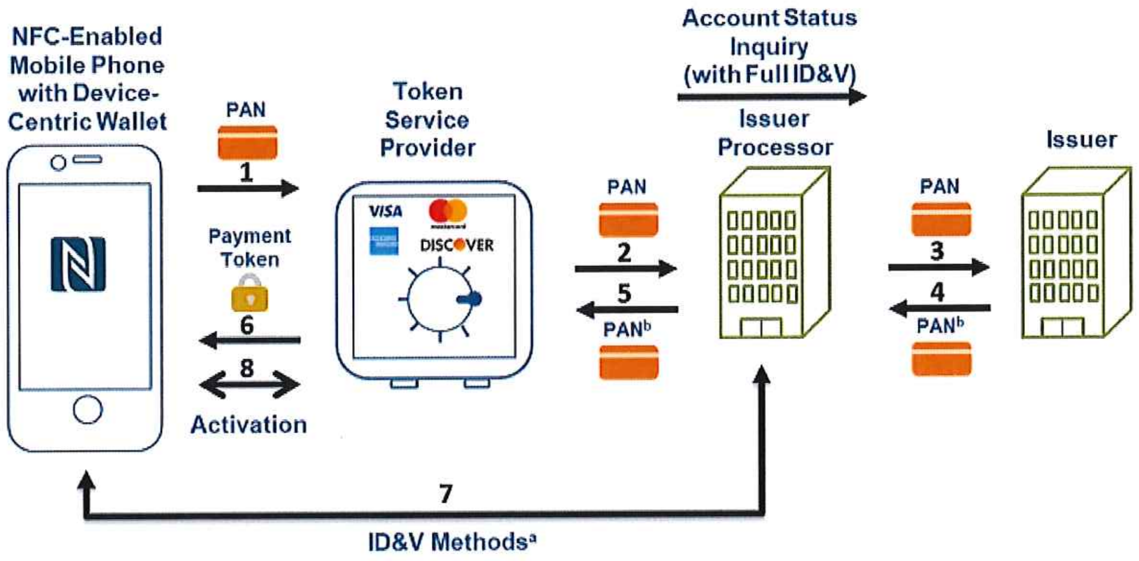
Card experience

We attract interest and build loyalty through branded material and digital DIY servicing tools. Secure payments can be made using Apple Pay, Google Pay, Samsung Pay with a phone, tablet or smart watch. Tap-to-pay is available wherever possible and contactless, payment-enabled credit cards are coming soon to meet the demands of our touch-free world.

(Source: https://www.elanfinancialservices.com/credit-card/what-we-offer/product-suites.html)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.

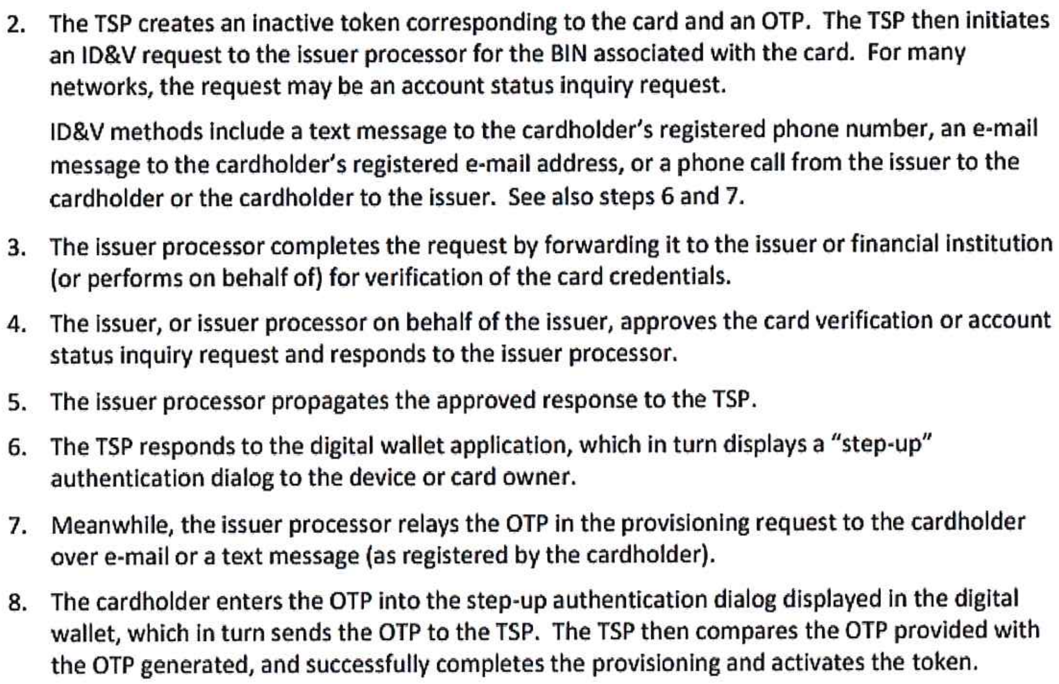


[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.



2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

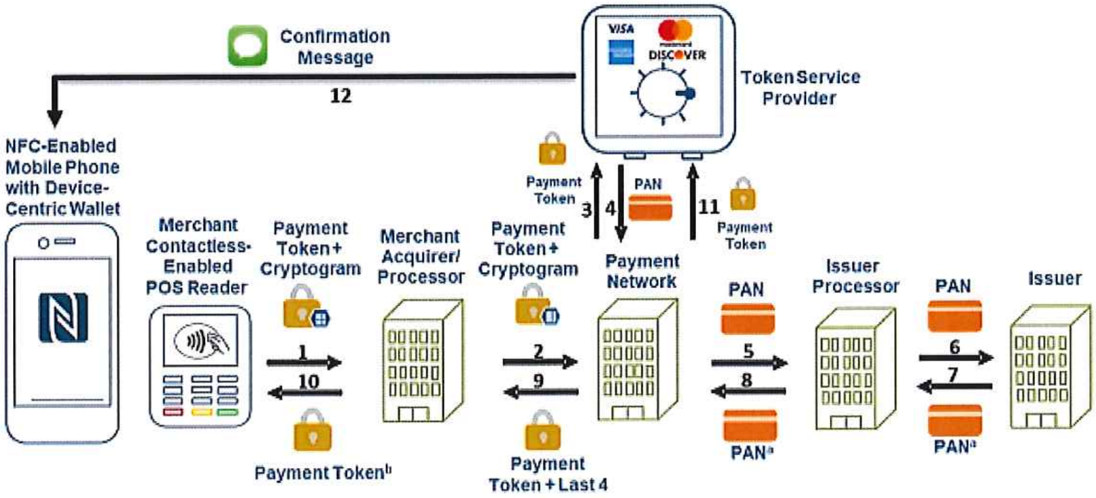
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

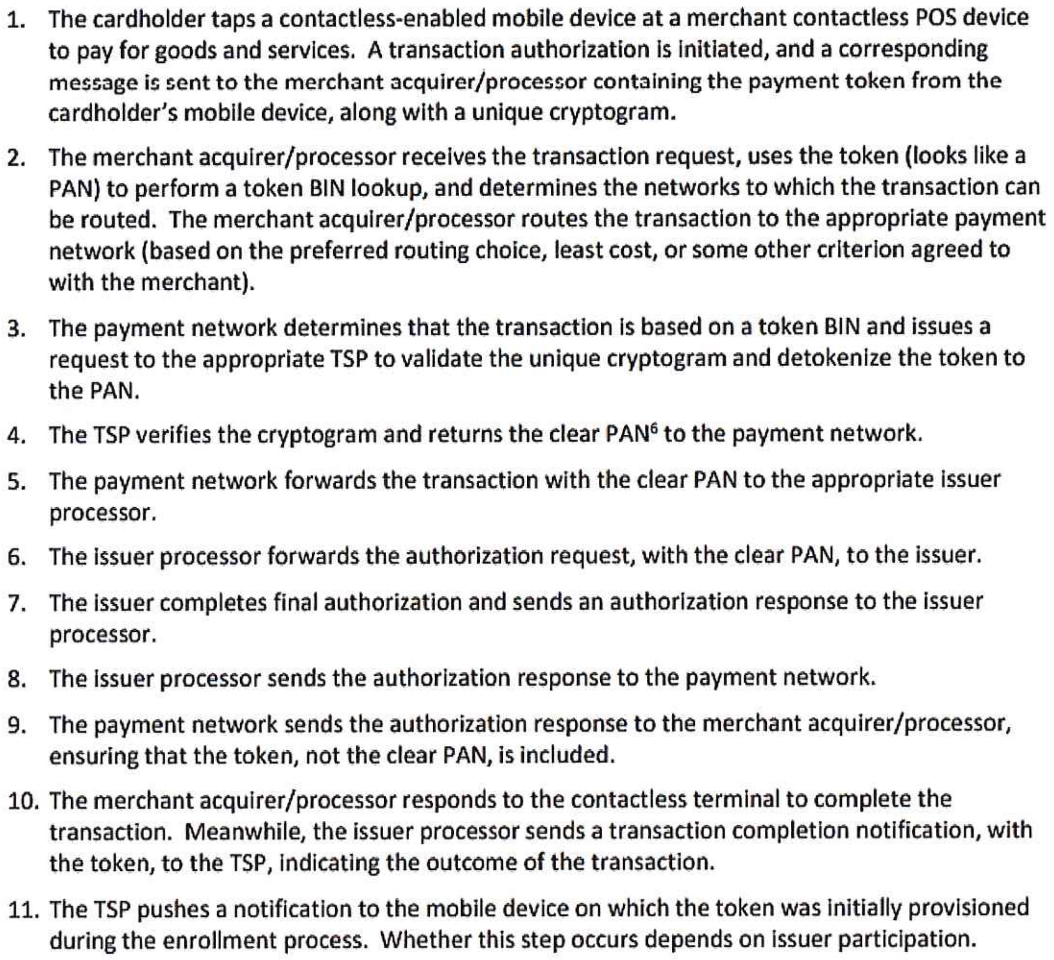


[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:



1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

62. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, an account holder of Defendant (or an account holder of a customer bank of Defendant) requests Defendant (or its customer bank) to provision a specific debit and/or credit card of Defendant (or its customer bank) for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her smartphone when

near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

63. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by a card holder of a debit and/or credit card of Defendant (or its customer bank) for provisioning a specific debit and/or credit card of a cardholder customer of Defendant (or its customer bank) for use on their mobile devices. This messaging gateway is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

64. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly

by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

65. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

66. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

67. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

68. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For

example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

69. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

70. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

71. Defendants have directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

72. In the pre-suit period, Comerica has indirectly infringed (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Comerica will continue to do so unless enjoined by this Court. Comerica's deliberate and/or willfully blind actions include,

but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Comerica knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

73. In the post-suit period, Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Defendants will continue to do so unless enjoined by this Court. Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing,

importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

74. In the pre-suit period, Comerica has made, used, made available for another's use, sold or offered to sell, the Accused Instrumentality, and/or has induced others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

75. In the post-suit period, Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

76. Defendants have committed these acts of infringement without license or authorization.

77. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

78. As a direct and proximate result of Defendants' infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

79. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at

law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

80. Comerica has had actual knowledge of the 802 Patent at least as of October 18, 2013, when Textile sent a letter to Ralph W. Babb, Jr., then Chief Executive Officer of Comerica Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

81. Comerica has had actual knowledge of the 802 Patent at least as of November 10, 2014, when Textile sent a letter to Ralph W. Babb, Jr., then Chief Executive Officer of Comerica Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

82. Defendants have had actual knowledge of the 802 Patent at least as of the dates when they were notified of the filing of this action. By the time of trial, Defendants will have known and intended (since receiving such notice) that their continued actions would infringe and actively induce the infringement of one or more claims of the 802 Patent.

83. In the pre-suit period, Comerica has also indirectly and willfully infringed the 802 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

84. In the post-suit period, Defendants have also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

85. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates

it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

86. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

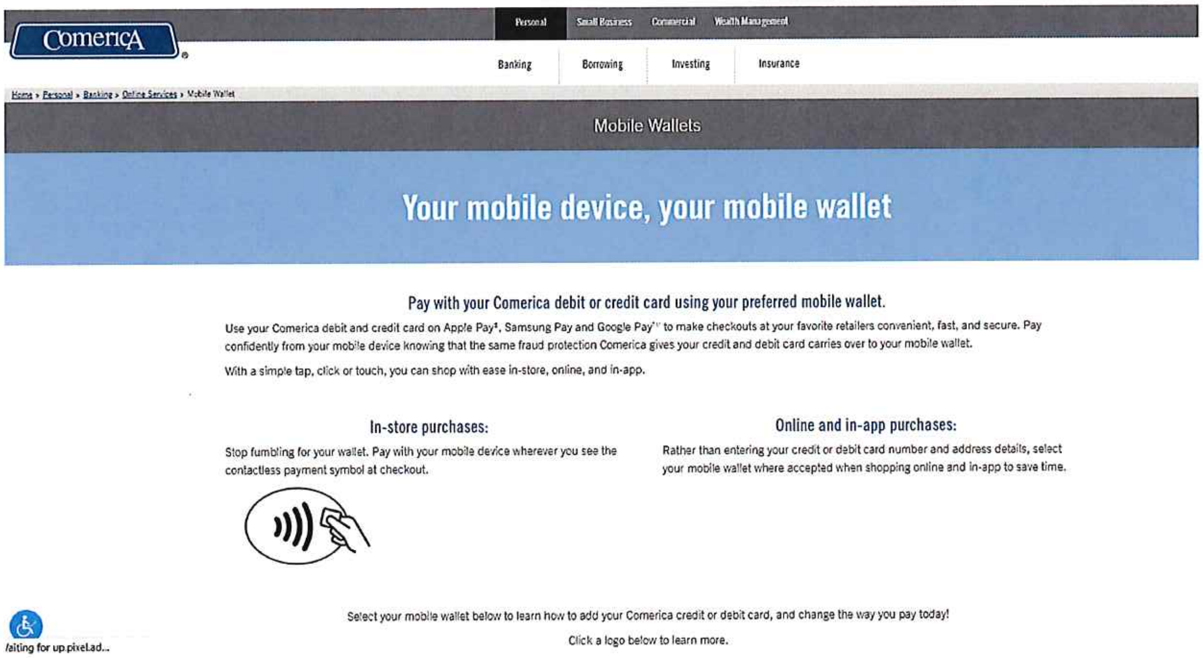
INFRINGEMENT OF U.S. PATENT NO. 9,584,499

87. On February 28, 2017, United States Patent No. 9,584,499 ("the 499 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Method."

88. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

89. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard and Visa Credit Card, that are used by Comerica in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the "Accused Instrumentality"). U.S. Bank offers debit and/or credit cards, such as the U.S. Bank Visa Debit Card and the U.S. Bank Visa Platinum Card, that are also used with the Accused Instrumentality card authentication system. U.S. Bank also provides services to other banks (including, but not limited to, Broadway National Bank, Comerica, Independent Bank, Southside Bank, and Texas Capital Bank) for the purposes of using the Accused Instrumentality card authentication system. The Accused Instrumentality transaction-specific access authentication systems that are used, made, and sold by Comerica and U.S. Bank are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit

card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Your mobile device, your mobile wallet

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay[1], Samsung Pay and Google Pay[TM] to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

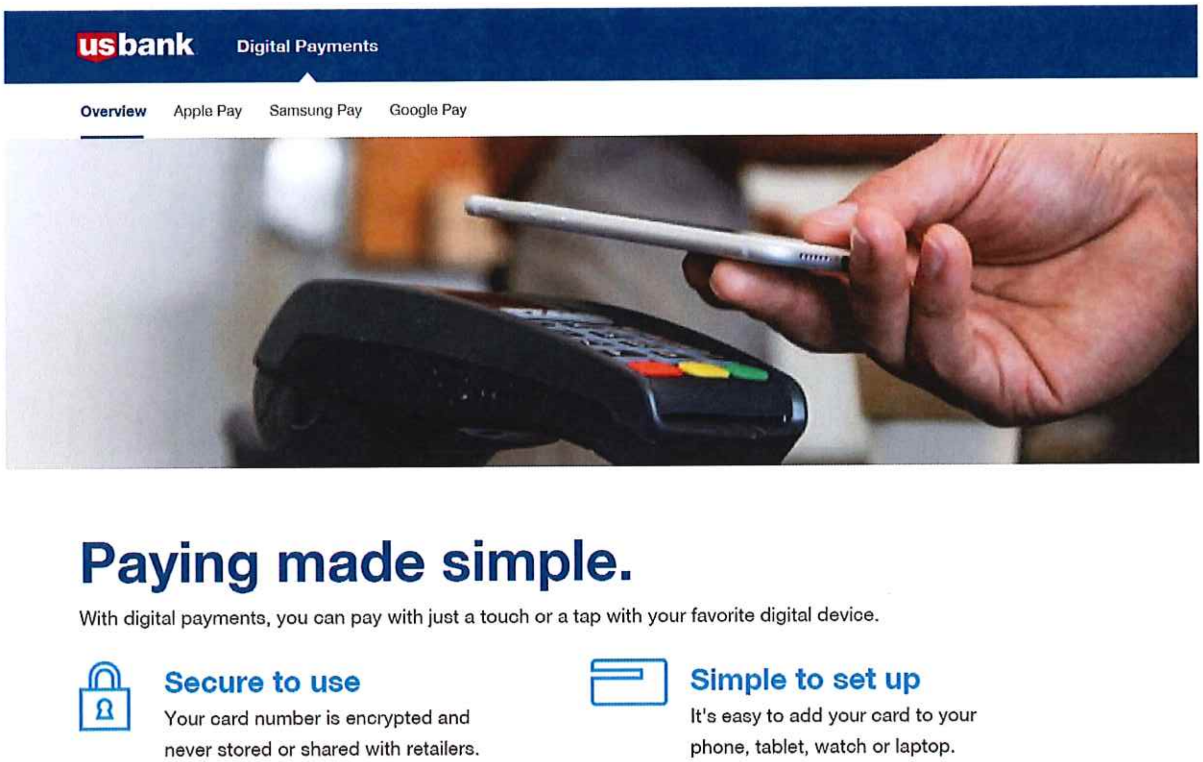
Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html)



Paying made simple.

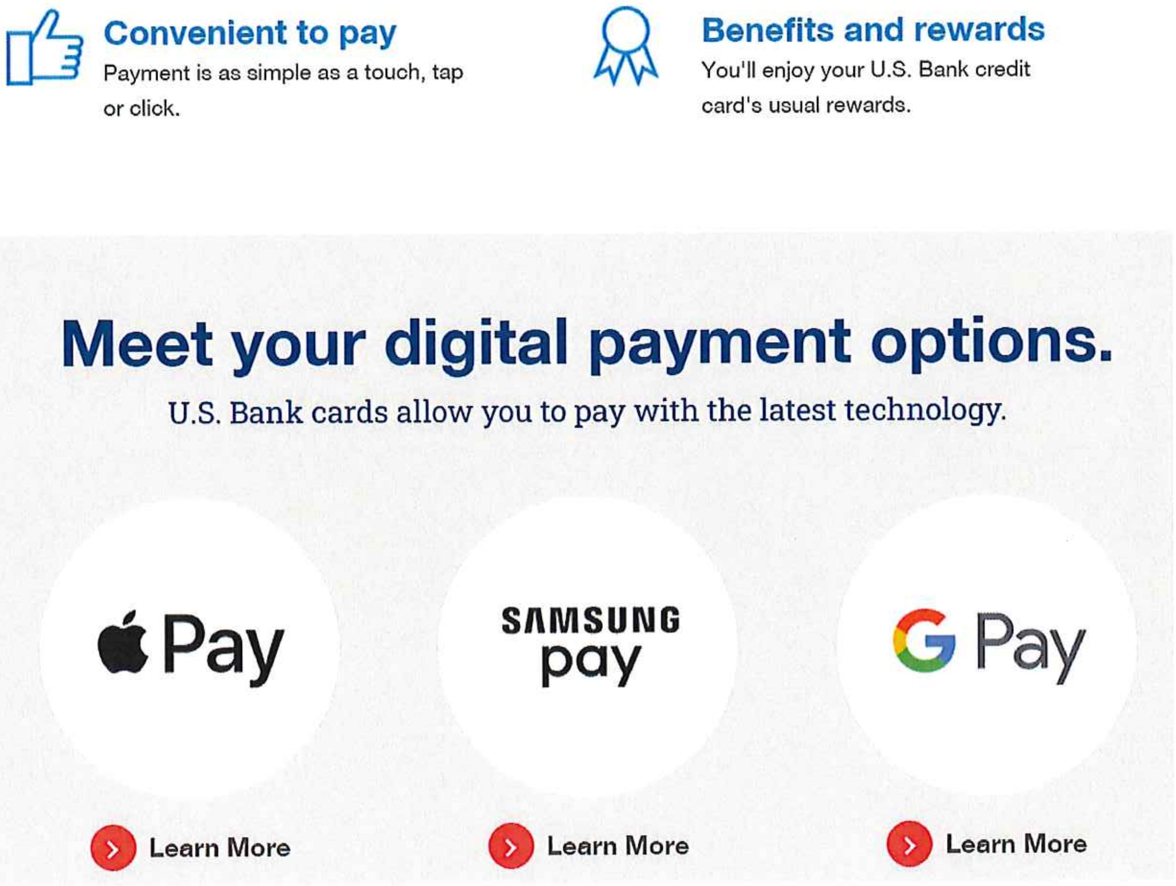
With digital payments, you can pay with just a touch or a tap with your favorite digital device.

Secure to use

Your card number is encrypted and never stored or shared with retailers.

Simple to set up

It's easy to add your card to your phone, tablet, watch or laptop.



Convenient to pay

Payment is as simple as a touch, tap or click.

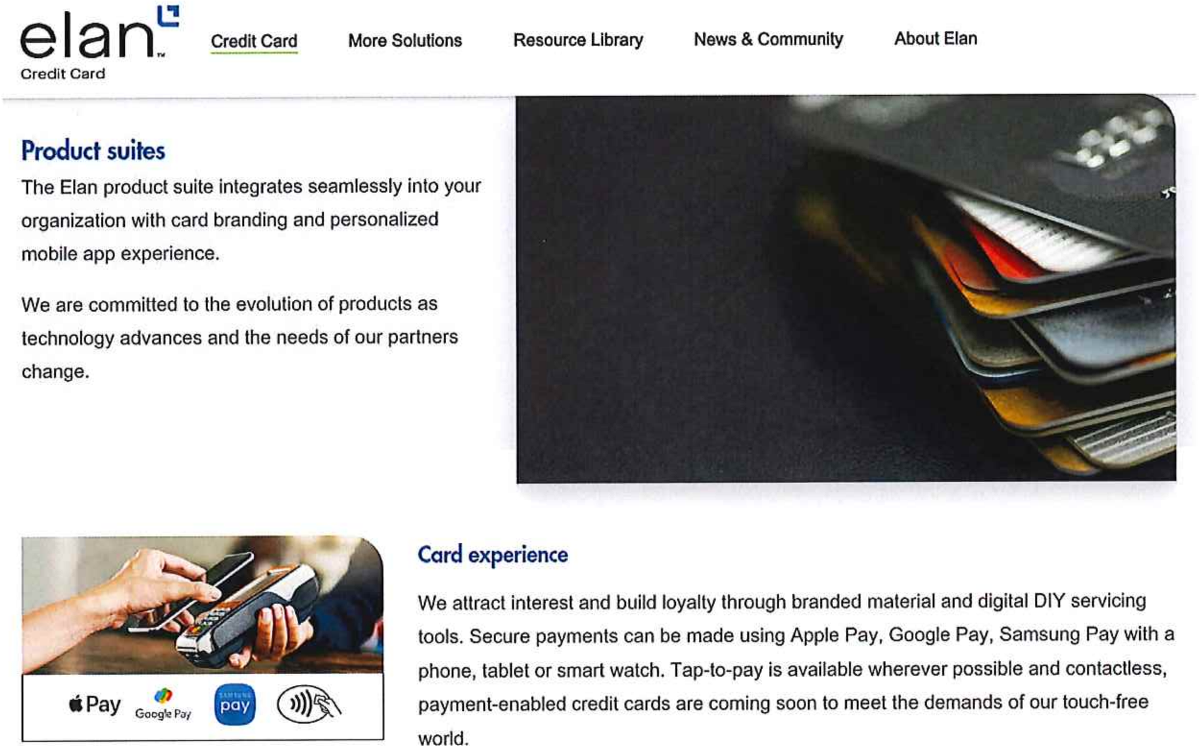
Benefits and rewards

You'll enjoy your U.S. Bank credit card's usual rewards.

Meet your digital payment options.

U.S. Bank cards allow you to pay with the latest technology.

(Source: https://www.usbankgomobile.com/wallet/#/home)



Product suites

The Elan product suite integrates seamlessly into your organization with card branding and personalized mobile app experience.

We are committed to the evolution of products as technology advances and the needs of our partners change.

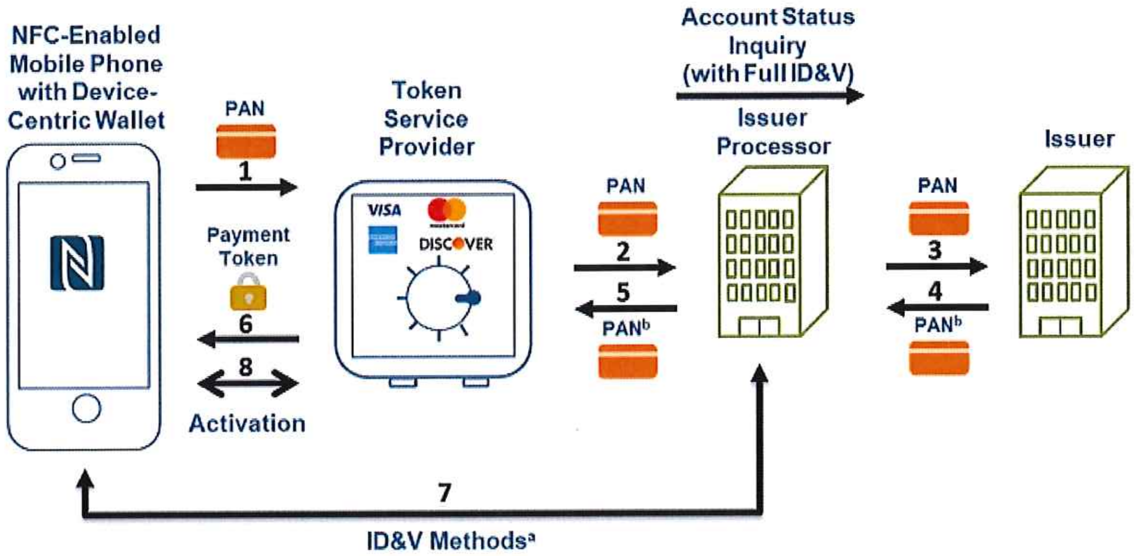
Card experience

We attract interest and build loyalty through branded material and digital DIY servicing tools. Secure payments can be made using Apple Pay, Google Pay, Samsung Pay with a phone, tablet or smart watch. Tap-to-pay is available wherever possible and contactless, payment-enabled credit cards are coming soon to meet the demands of our touch-free world.

(Source: https://www.elanfinancialservices.com/credit-card/what-we-offer/product-suites.html)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.

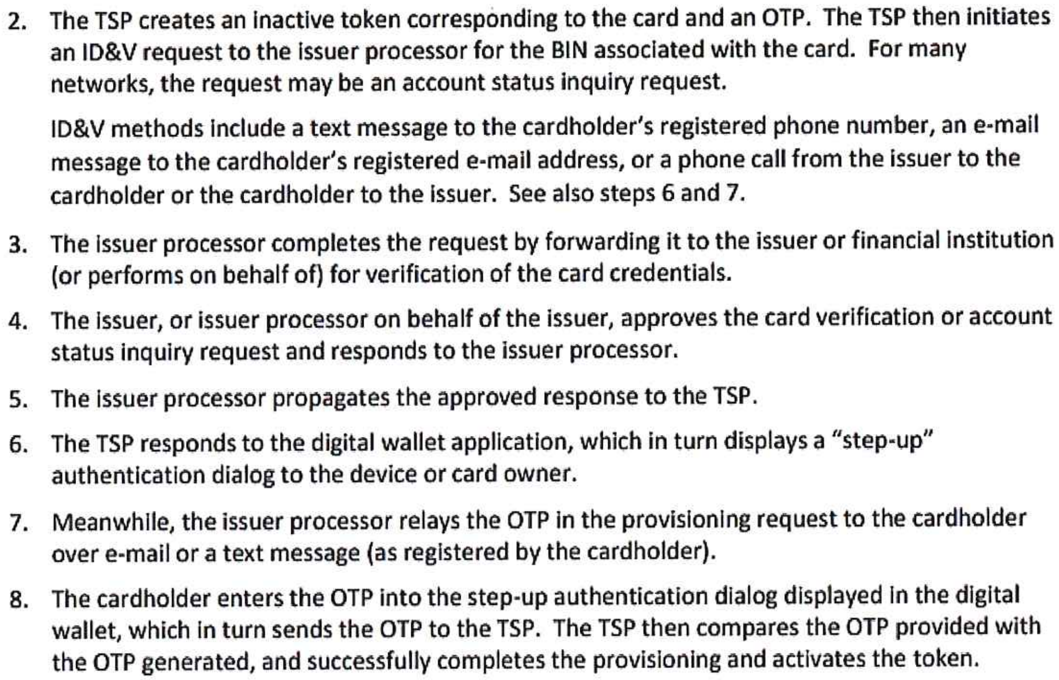


[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.



2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.

4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.

5. The issuer processor propagates the approved response to the TSP.

6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.

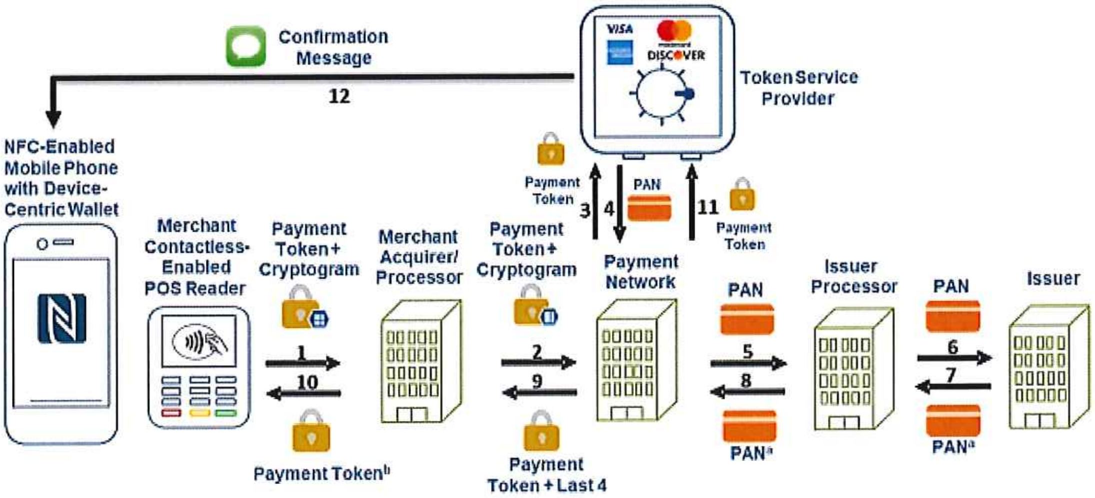
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).

8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

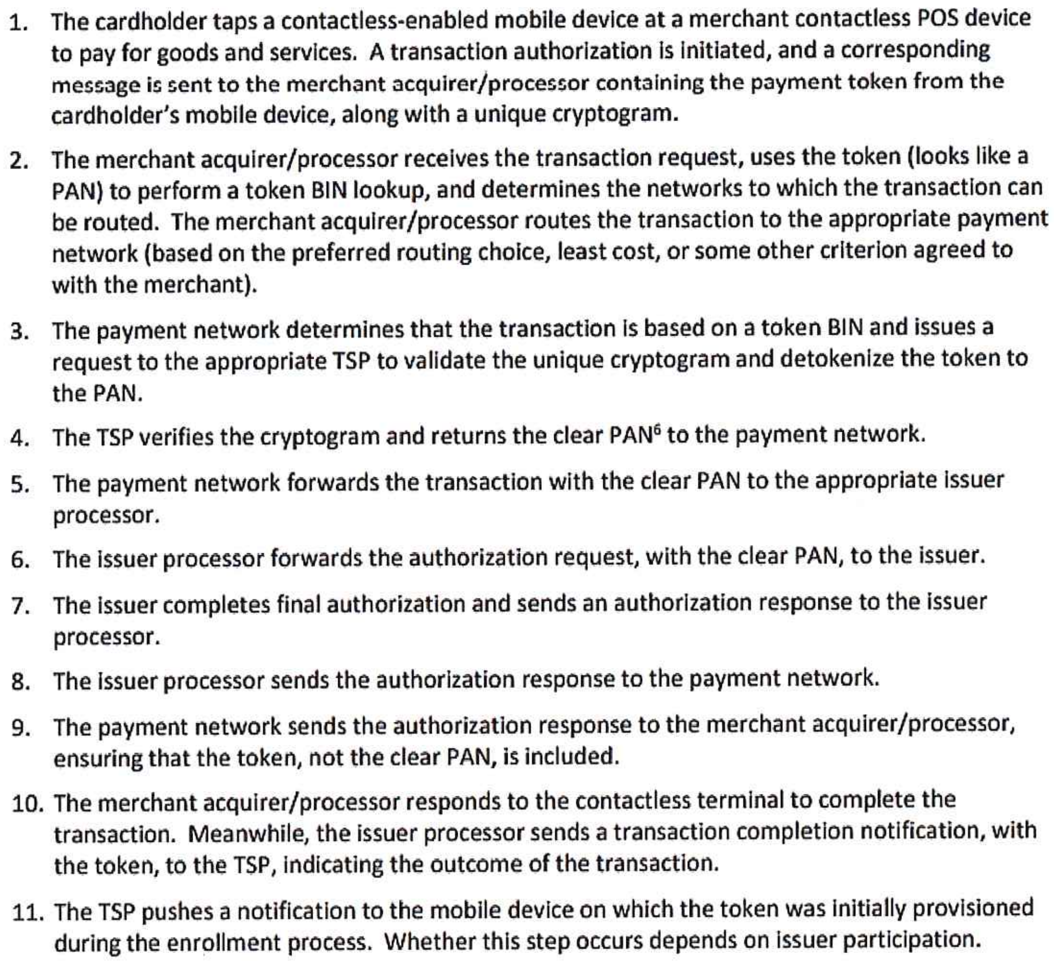
Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:



1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

90. Defendants' use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, an account holder of Defendant (or an account holder of a customer bank of Defendant) requests Defendant (or its customer bank) to provision a specific debit and/or credit card of Defendant (or its customer bank) for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her smartphone when

near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

91. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by a cardholder customer of Defendant (or its customer bank) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of a cardholder customer of Defendant (or its customer bank). This messaging gateway is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

92. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string.

For example, behind the firewall of the messaging gateway and in communication therewith is an authorization server that generates a token corresponding to a secured resource during the provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

93. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

94. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services. The authorization server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

95. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by said authorized user. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

96. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

97. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

98. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

99. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

100. Defendants have directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

101. In the post-suit period, Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Defendants will continue to do so unless enjoined by this Court. Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing,

importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

102. In the post-suit period, Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

103. Defendants have committed these acts of infringement without license or authorization.

104. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

105. As a direct and proximate result of Defendants' infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

106. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

107. Defendants have had actual knowledge of the 499 Patent at least as of the date when they were notified of the filing of this action. By the time of trial, Defendants will have known and intended (since receiving such notice) that their continued actions would infringe and actively induce the infringement of one or more claims of the 499 Patent.

108. In the post-suit period, Defendants have also indirectly and willfully infringed, and continue to indirectly and willfully infringe, the 499 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

109. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

110. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.

COUNT IV

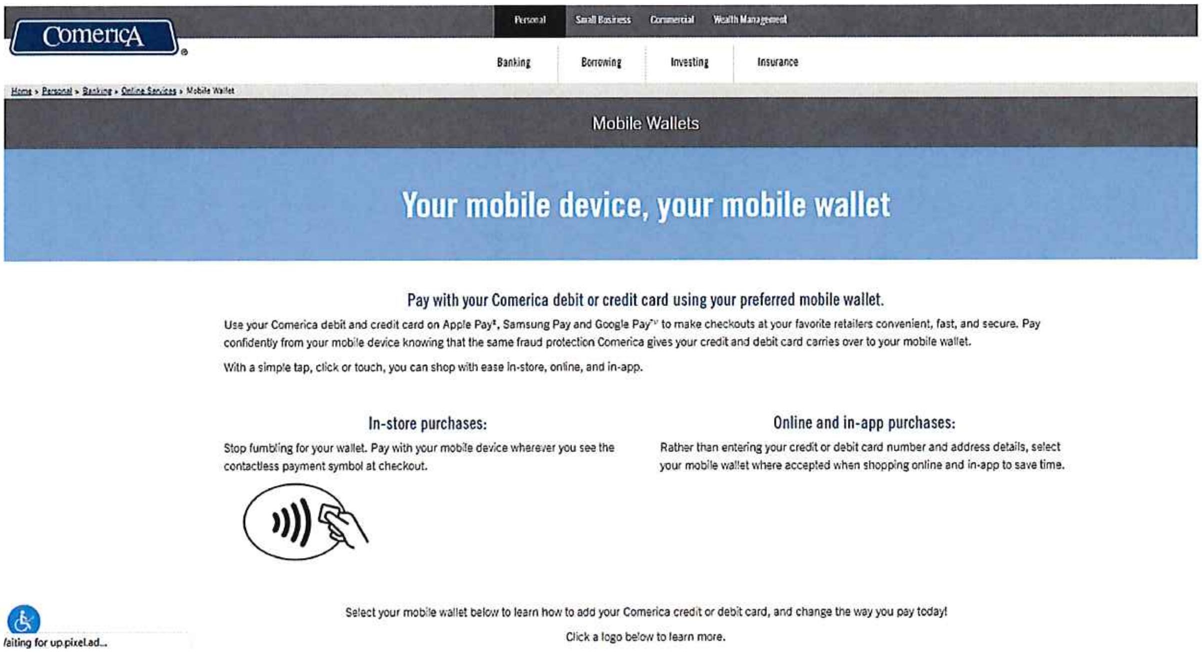
INFRINGEMENT OF U.S. PATENT NO. 10,148,659

111. On December 4, 2018, United States Patent No. 10,148,659 ("the 659 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Method."

112. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

113. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard and Visa Credit Card, that are used with a computer-implemented system for a credit or debit

and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the "Accused Instrumentality"). U.S. Bank offers debit and/or credit cards, such as the U.S. Bank Visa Debit Card and the U.S. Bank Visa Platinum Card, that are also used with the Accused Instrumentality card authentication system. U.S. Bank also provides services to other banks (including, but not limited to, Broadway National Bank, Comerica, Independent Bank, Southside Bank, and Texas Capital Bank) for the purposes of using the Accused Instrumentality card authentication system. The Accused Instrumentality transaction-specific access authentication systems that are used, made, and sold by Comerica and U.S. Bank are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Mobile Wallets

Your mobile device, your mobile wallet

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay[2], Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

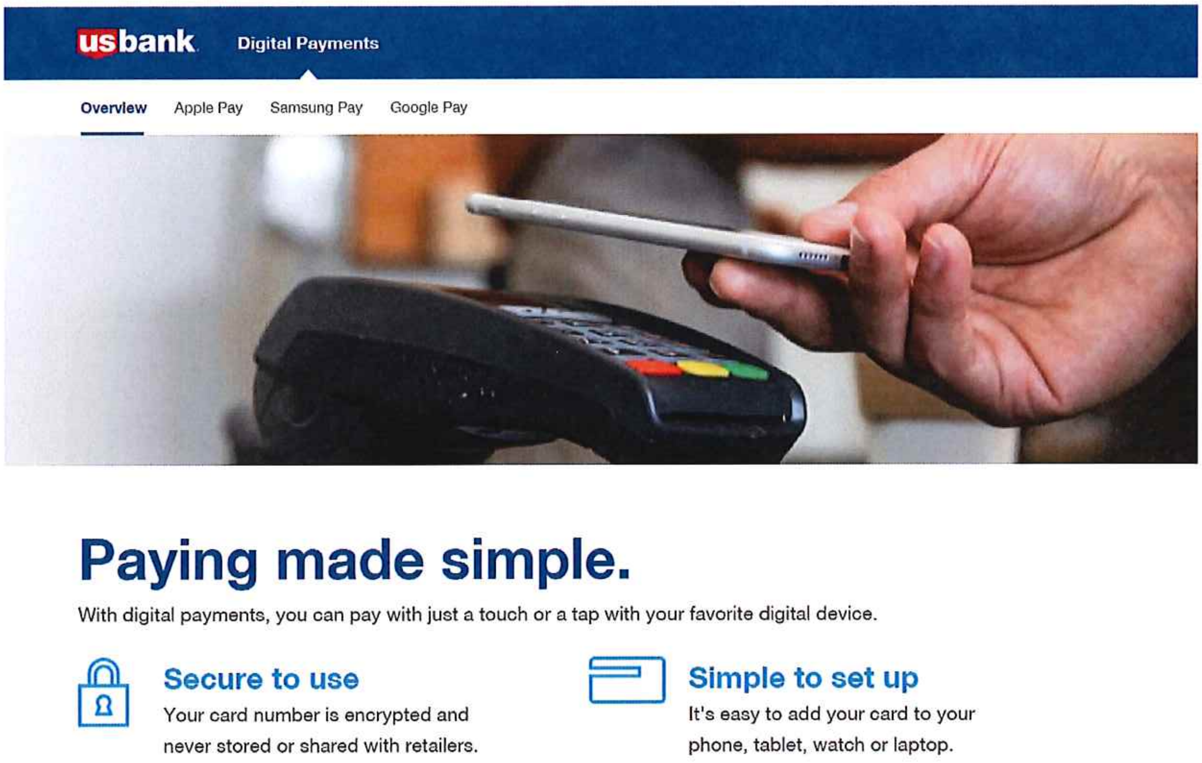
Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html)



Paying made simple.

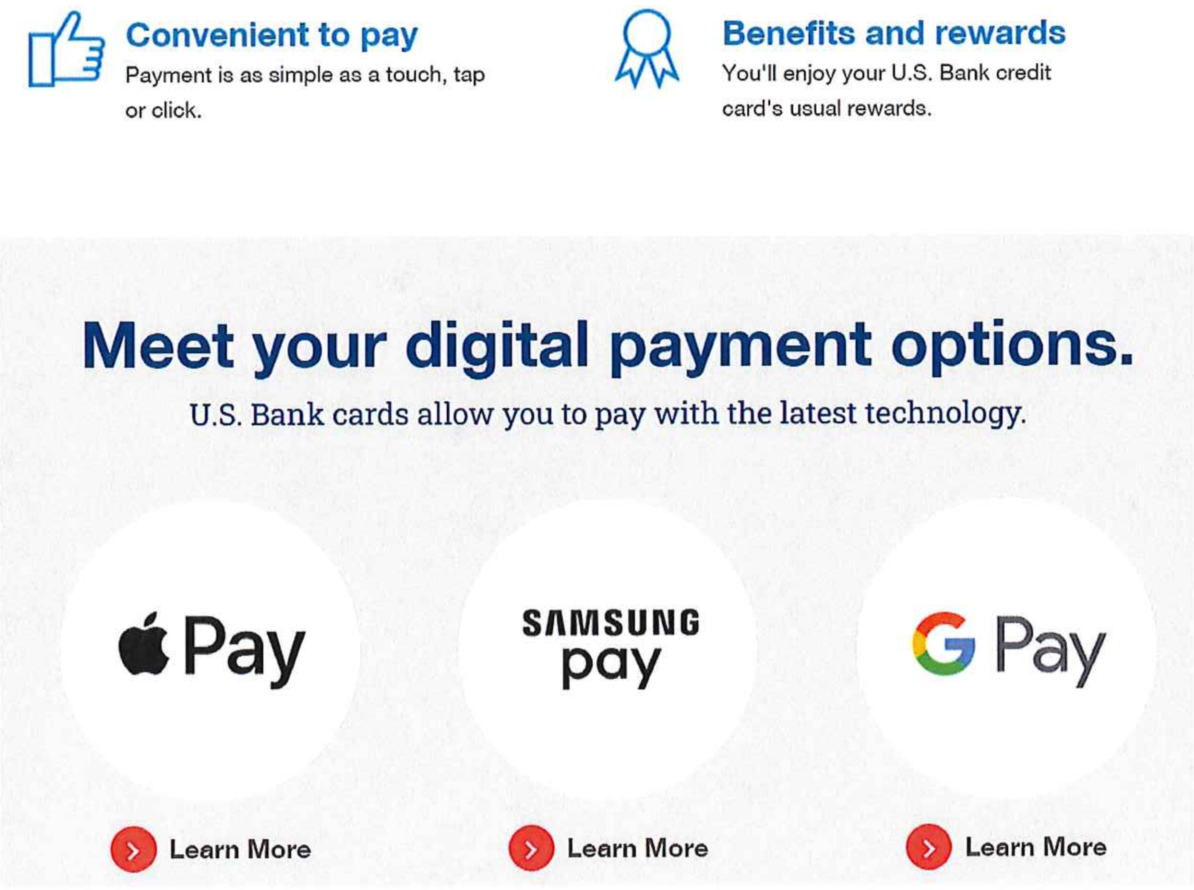
With digital payments, you can pay with just a touch or a tap with your favorite digital device.

Secure to use

Your card number is encrypted and never stored or shared with retailers.

Simple to set up

It's easy to add your card to your phone, tablet, watch or laptop.



Convenient to pay

Payment is as simple as a touch, tap or click.

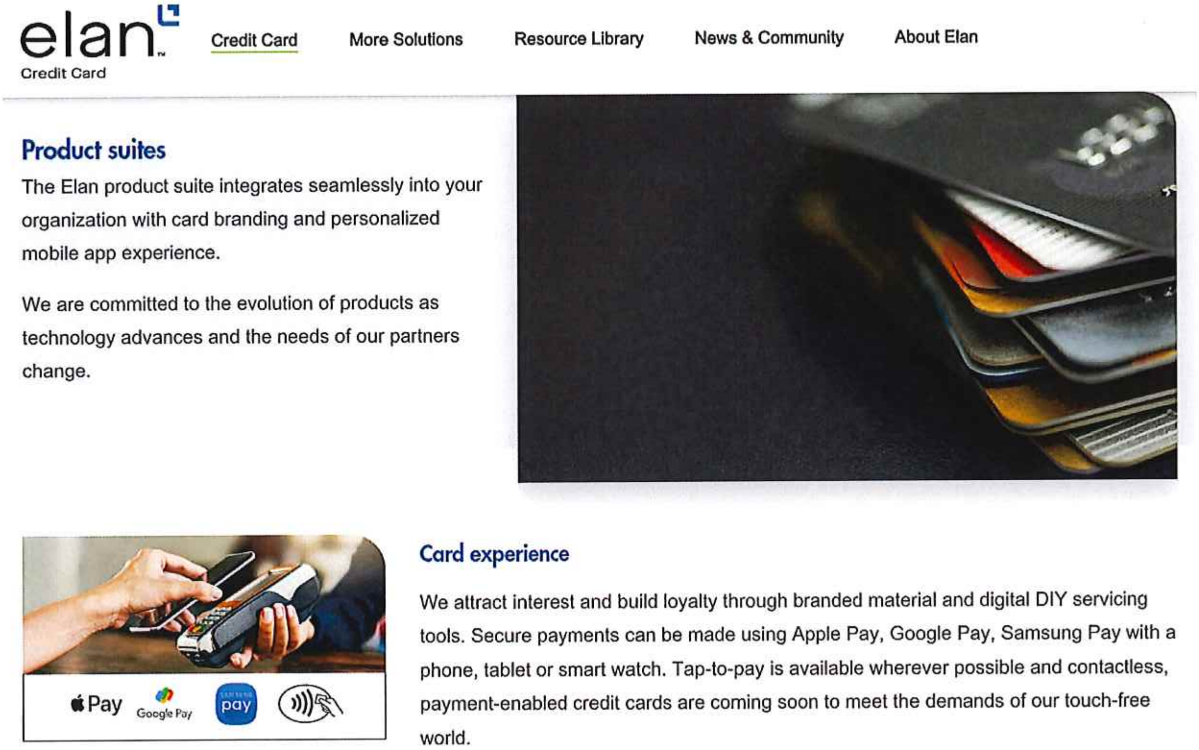
Benefits and rewards

You'll enjoy your U.S. Bank credit card's usual rewards.

Meet your digital payment options.

U.S. Bank cards allow you to pay with the latest technology.

(Source: https://www.usbankgomobile.com/wallet/#/home)



Product suites

The Elan product suite integrates seamlessly into your organization with card branding and personalized mobile app experience.

We are committed to the evolution of products as technology advances and the needs of our partners change.

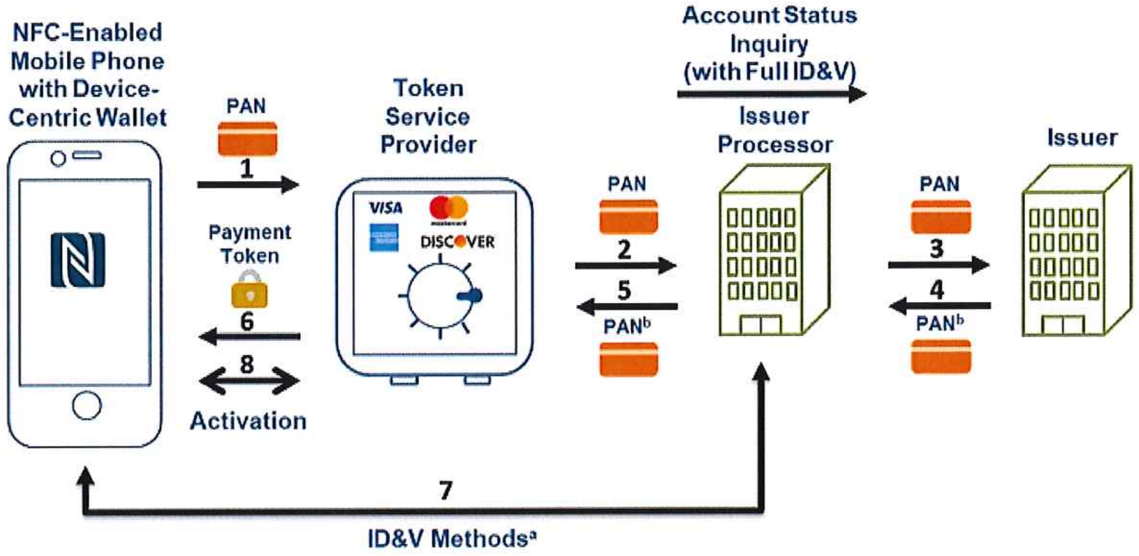
Card experience

We attract interest and build loyalty through branded material and digital DIY servicing tools. Secure payments can be made using Apple Pay, Google Pay, Samsung Pay with a phone, tablet or smart watch. Tap-to-pay is available wherever possible and contactless, payment-enabled credit cards are coming soon to meet the demands of our touch-free world.

(Source: https://www.elanfinancialservices.com/credit-card/what-we-offer/product-suites.html)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.

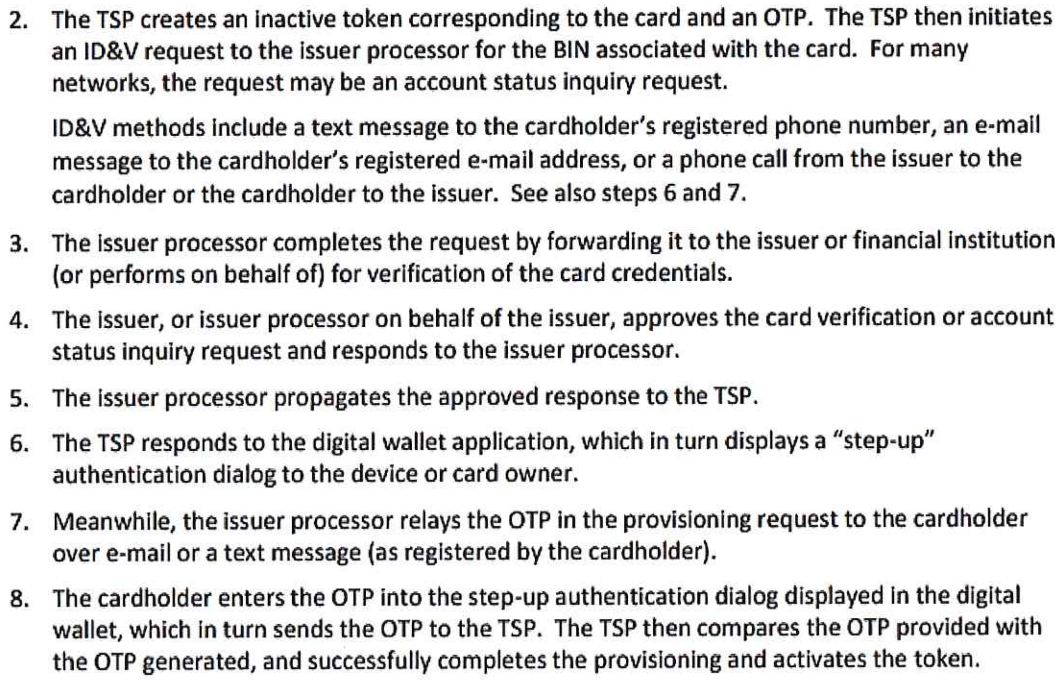


[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.



2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

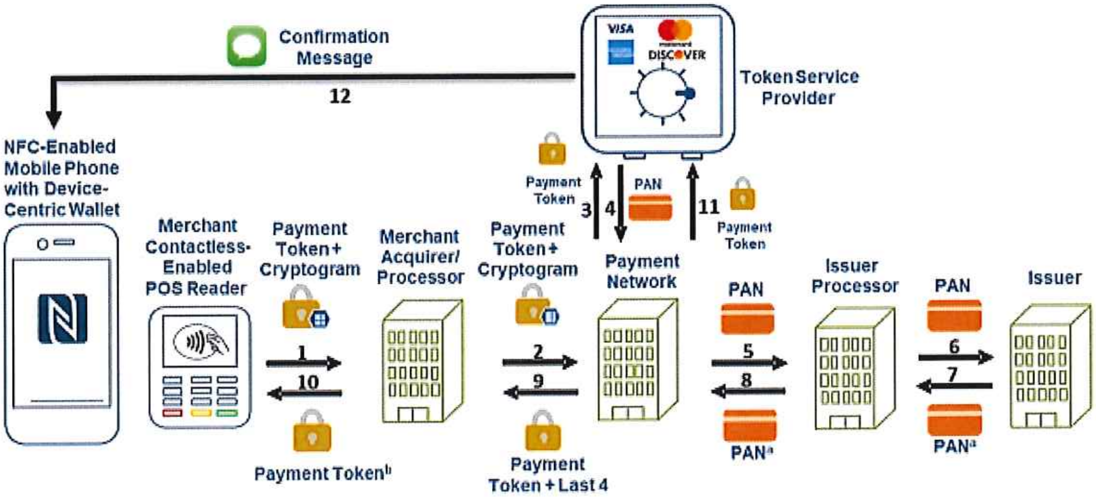
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

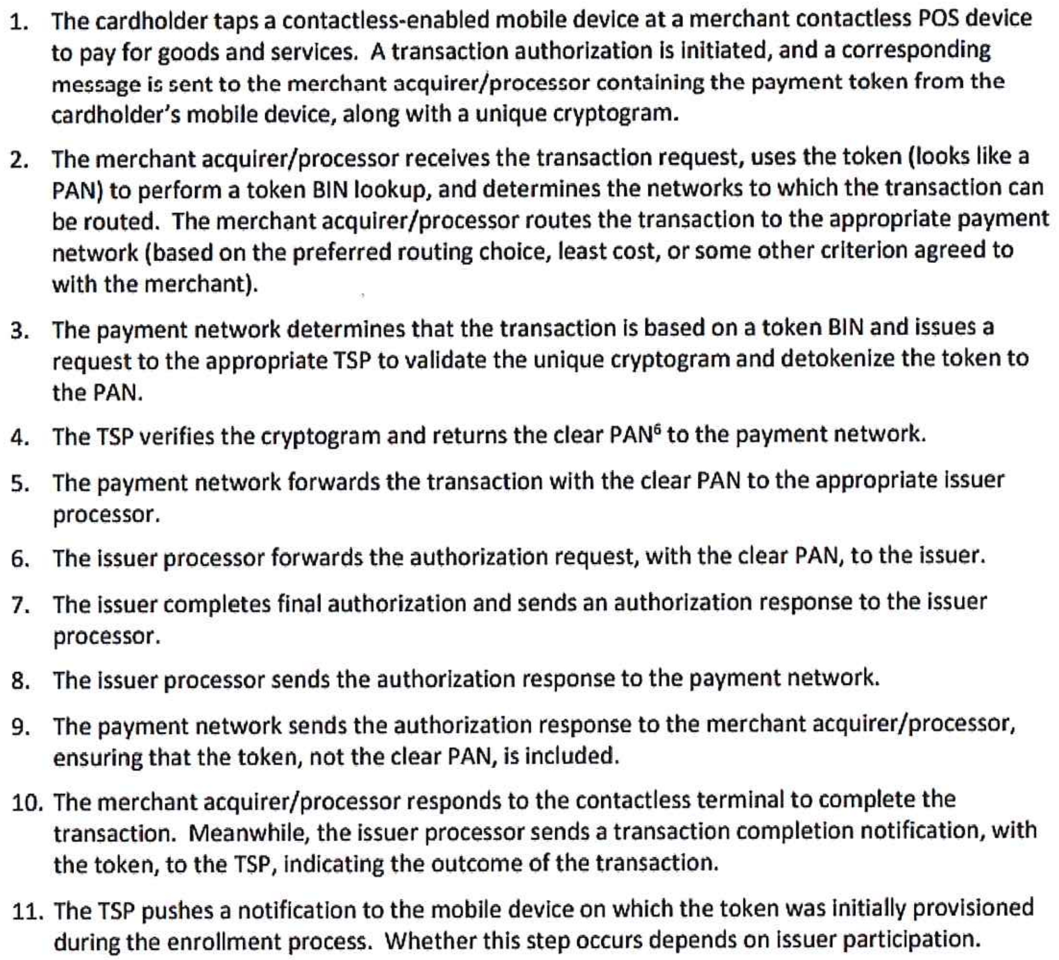


[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:



1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

114. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, an account holder of Defendant (or an account holder of a customer bank of Defendant) requests Defendant (or its customer bank) to provision a specific debit and/or credit card of Defendant (or its customer bank) for use on his or her mobile device. The account holder can then request for

payment to be made by Defendant (or its customer bank) to a specific merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

115. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with an account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by a cardholder customer of Defendant (or its customer bank) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of a cardholder customer of Defendant (or its customer bank). This interface is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

116. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction

embodied in a computer readable medium, the first instruction operable to receive registration information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from account holders through the interface for provisioning a specific debit and/or credit card of Defendant (or its customer bank) for use on their mobile devices. The server is also programmed to receive requests initiated by a cardholder customer of Defendant (or its customer bank) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of a cardholder customer of Defendant (or its customer bank). The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

117. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference

identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the account holder's mobile device. The server is programmed to receive authorization requests initiated by an account holder for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the account holder identifier. The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

118. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

119. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the account holder's mobile device. The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

120. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

121. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

122. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

123. Defendants have directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35

U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

124. In the post-suit period, Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Defendants will continue to do so unless enjoined by this Court. Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

125. In the post-suit period, Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

126. Defendants have committed these acts of infringement without license or authorization.

127. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

128. As a direct and proximate result of Defendants' infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

129. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

130. Defendants have had actual knowledge of the 659 Patent at least as of the date when they were notified of the filing of this action. By the time of trial, Defendants will have known and intended (since receiving such notice) that their continued actions would infringe and actively induce the infringement of one or more claims of the 659 Patent.

131. In the post-suit period, Defendants have also indirectly and willfully infringed, and continue to indirectly and willfully infringe, the 659 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

132. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

133. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

COUNT V

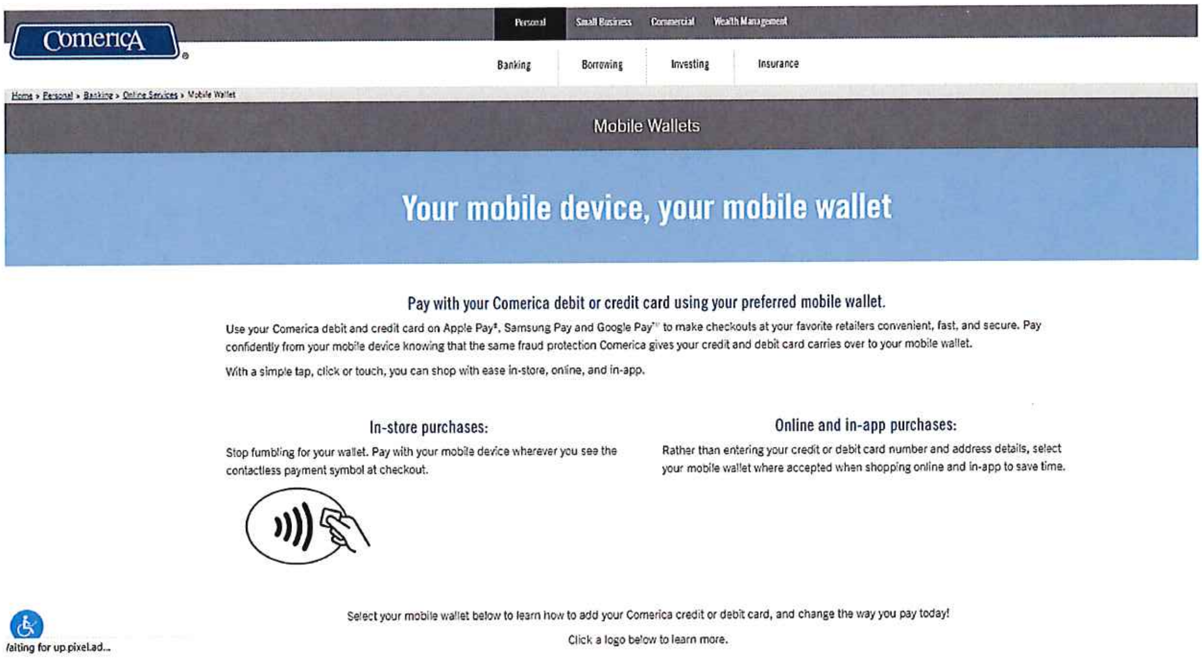
INFRINGEMENT OF U.S. PATENT NO. 10,560,454

134. On February 11, 2020, United States Patent No. 10,560,454 ("the 454 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Method."

135. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

136. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard and Visa Credit Card, that are used with a computer-implemented system for a user to authorize a resource authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client (the "Accused Instrumentality"). U.S. Bank offers debit and/or credit cards, such as the U.S. Bank Visa Debit Card and the U.S. Bank Visa Platinum Card, that are also used with the Accused Instrumentality card authentication system. U.S. Bank also provides services to other banks (including, but not limited to, Broadway National Bank, Comerica, Independent Bank, Southside Bank, and Texas Capital Bank) for the purposes of using the Accused

Instrumentality card authentication system. The Accused Instrumentality transaction-specific access authentication systems that are used, made, and sold by Comerica and U.S. Bank are implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.


Comerica
Personal
Small Business
Commercial
Wealth Management
Banking
Borrowing
Investing
Insurance
Home › Personal › Banking › Online Services › Mobile Wallet
Mobile Wallets
Your mobile device, your mobile wallet
Waiting for up.pixel.ad...

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay®, Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

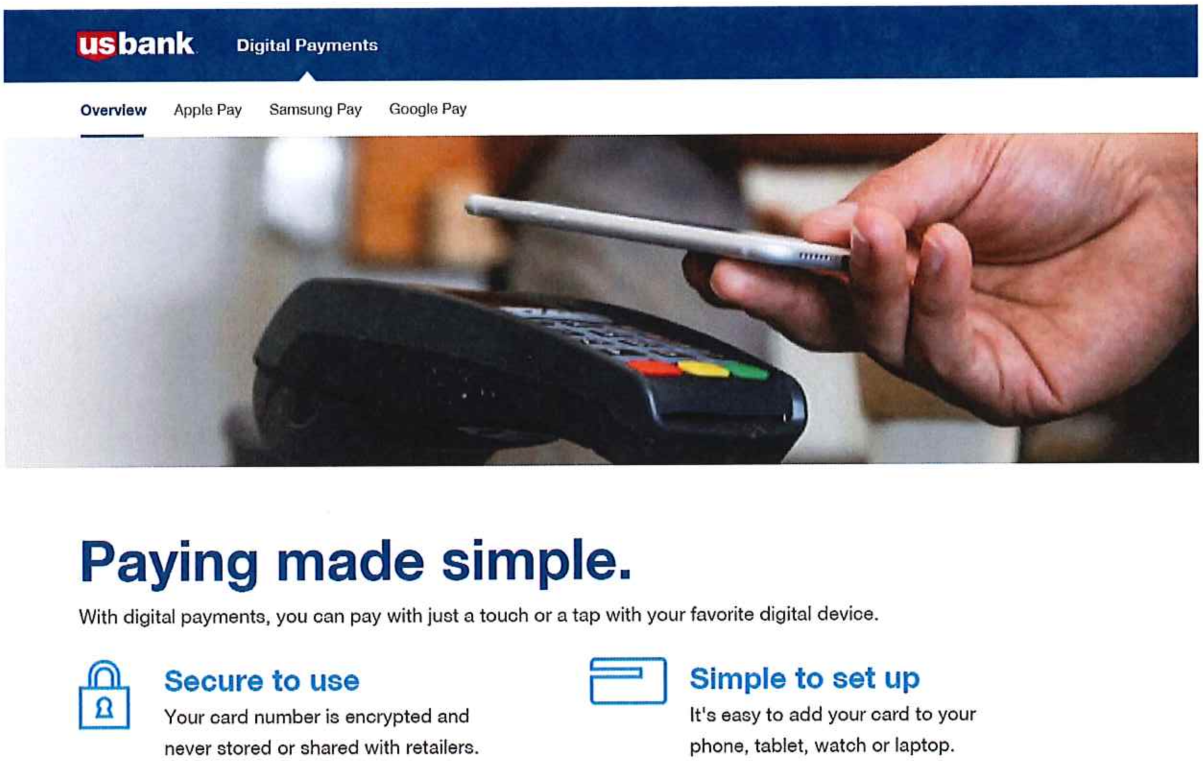
Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html)



Paying made simple.

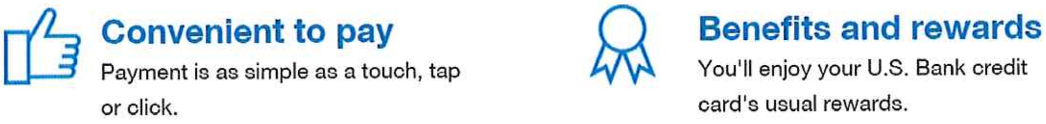
With digital payments, you can pay with just a touch or a tap with your favorite digital device.

Secure to use

Your card number is encrypted and never stored or shared with retailers.

Simple to set up

It's easy to add your card to your phone, tablet, watch or laptop.

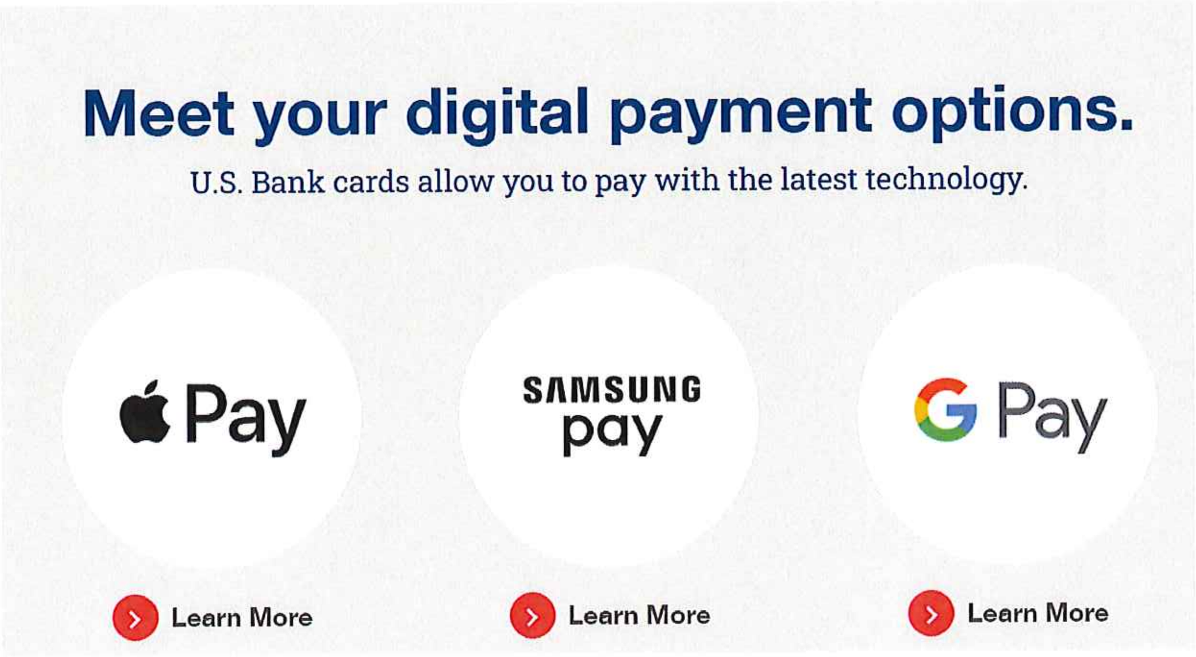


Convenient to pay

Payment is as simple as a touch, tap or click.

Benefits and rewards

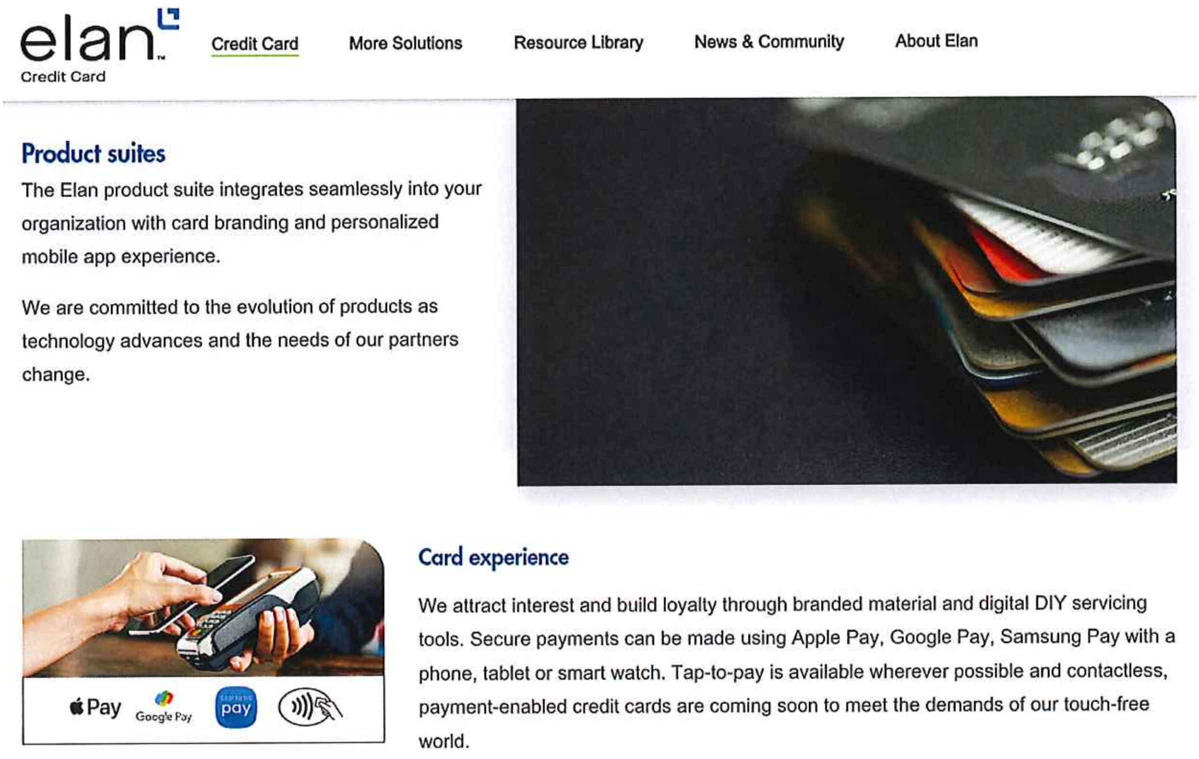
You'll enjoy your U.S. Bank credit card's usual rewards.



Meet your digital payment options.

U.S. Bank cards allow you to pay with the latest technology.

(Source: https://www.usbankgomobile.com/wallet/#/home)



Product suites

The Elan product suite integrates seamlessly into your organization with card branding and personalized mobile app experience.

We are committed to the evolution of products as technology advances and the needs of our partners change.

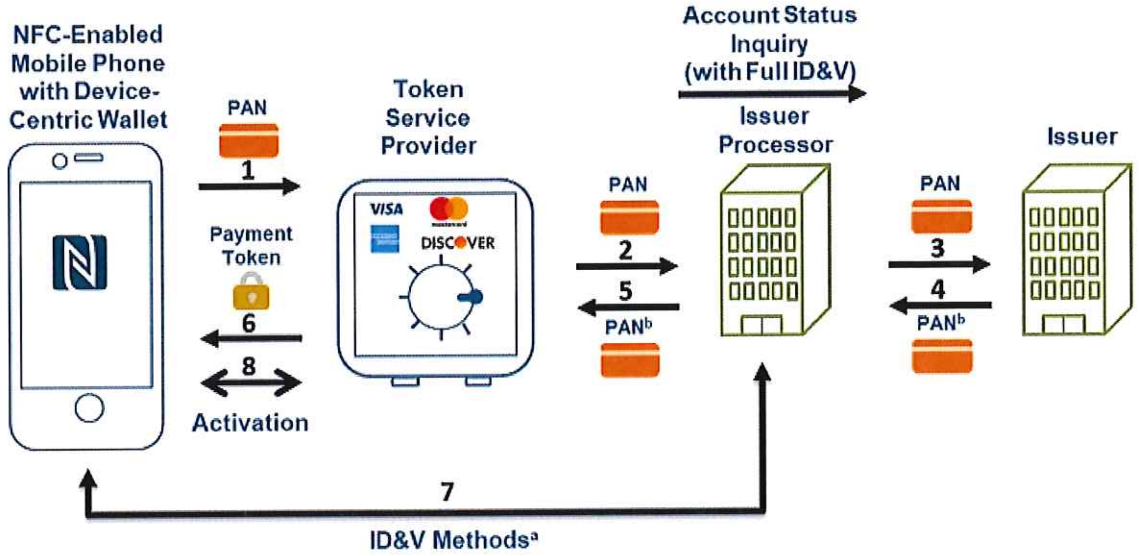
Card experience

We attract interest and build loyalty through branded material and digital DIY servicing tools. Secure payments can be made using Apple Pay, Google Pay, Samsung Pay with a phone, tablet or smart watch. Tap-to-pay is available wherever possible and contactless, payment-enabled credit cards are coming soon to meet the demands of our touch-free world.

(Source: https://www.elanfinancialservices.com/credit-card/what-we-offer/product-suites.html)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.

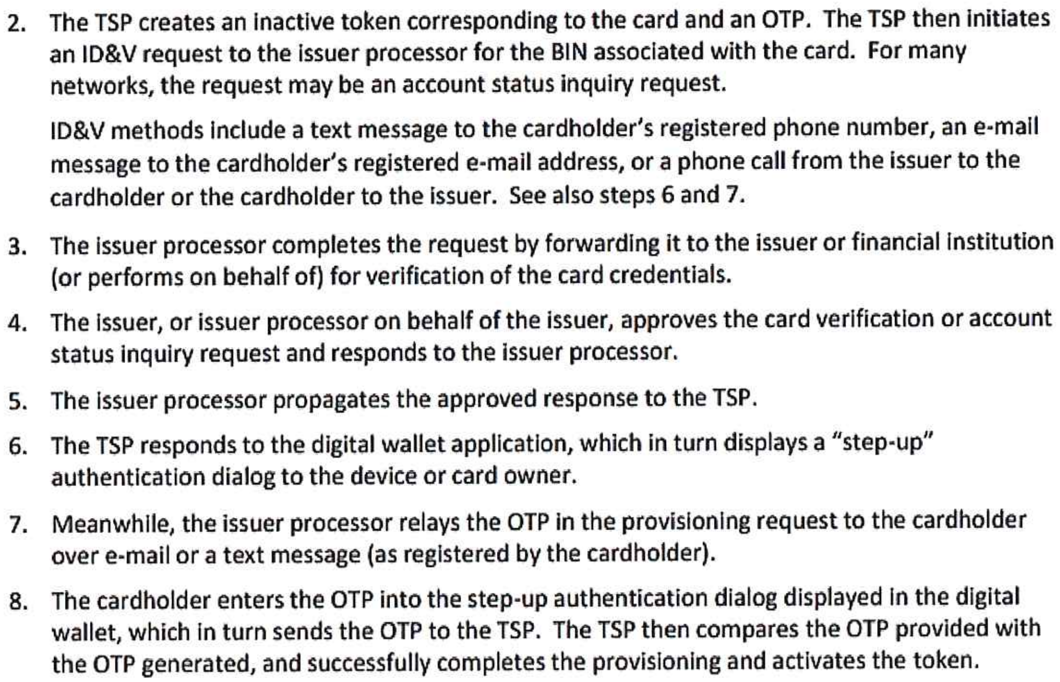


[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.



2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

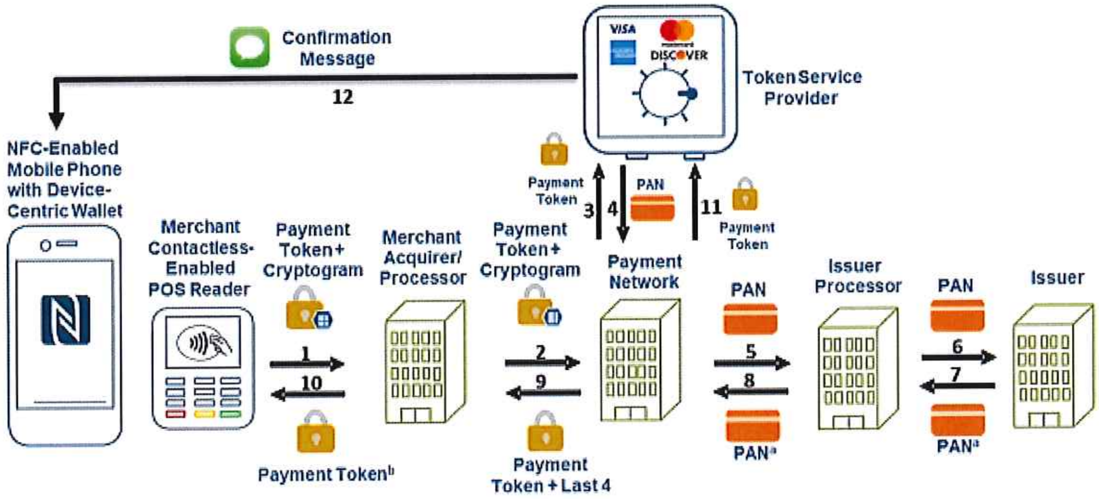
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

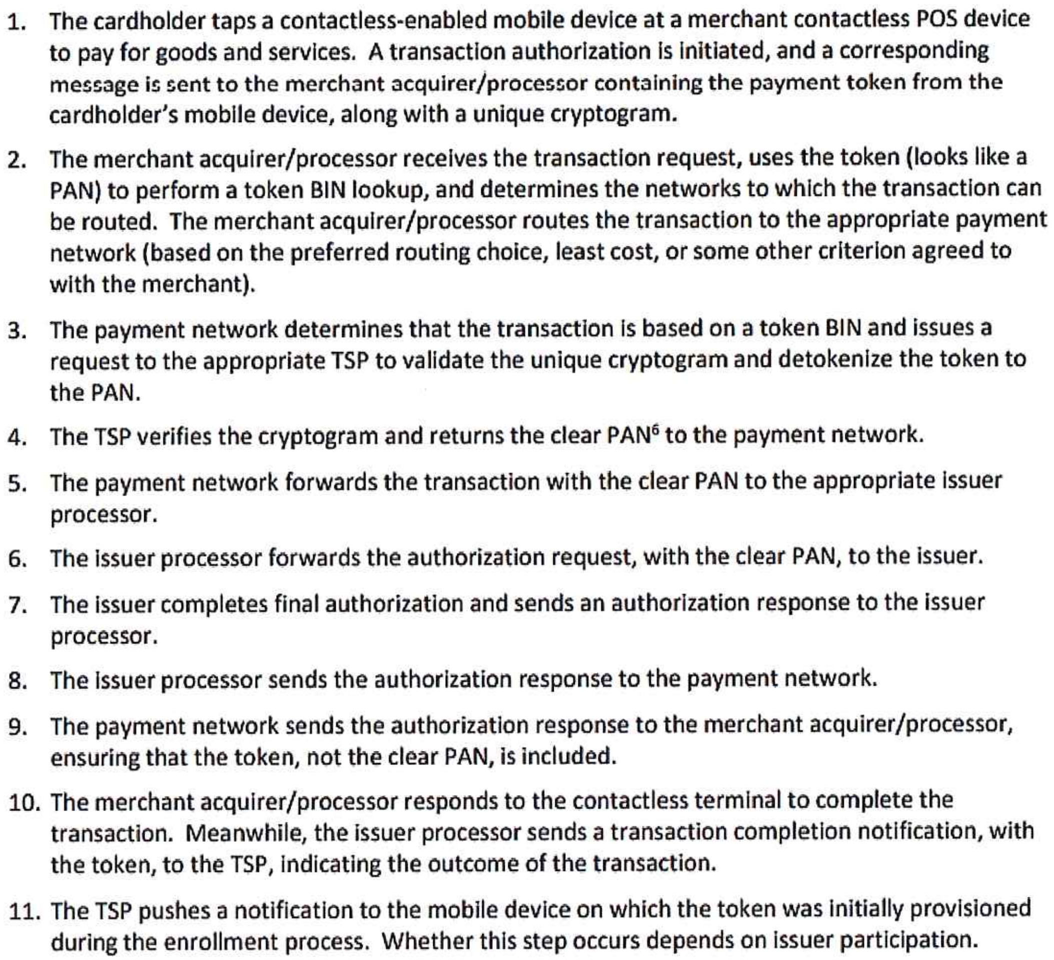
Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:



1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

137. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, an account holder of Defendant (or an account holder of a customer bank of Defendant) requests Defendant (or its customer bank) to provision a specific debit and/or credit card of Defendant (or its customer bank) for use on his or her mobile device. The account holder can then request for payment to be made by Defendant (or its customer bank) to a specific

merchant in a specific amount for a specific transaction from a specific card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

138. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with an account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by a cardholder customer of Defendant (or its customer bank) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of a cardholder customer of Defendant (or its customer bank). This interface is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

139. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction

embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from account holders through the interface for provisioning a specific debit and/or credit card of Defendant (or its customer bank) for use on their mobile devices. The server is also programmed to receive requests initiated by a cardholder customer of Defendant (or its customer bank) for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific card account of a cardholder customer of Defendant (or its customer bank). The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

140. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message

having been received through the at least one interface and originating from the account holder's mobile device. The server is programmed to receive authorization requests initiated by an account holder for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a CVV number, a merchant identifier, other token information, and the account holder identifier. The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

141. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

142. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access

request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the account holder's mobile device. The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to receive the messages.

143. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment

request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Defendant or through an agent with whom Defendant has contracted to provide the authentication services.

144. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

145. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendants' use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

146. Defendants have directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

147. In the post-suit period, Defendants have indirectly infringed and continue to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Defendants will continue to do so unless enjoined by this Court.

Defendants' deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Defendants knew and/or were willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

148. In the post-suit period, Defendants continue to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continue to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

149. Defendants have committed these acts of infringement without license or authorization.

150. By engaging in the conduct described herein, Defendants have caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Defendants are thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

151. As a direct and proximate result of Defendants' infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount

adequate to compensate Textile for Defendants' past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

152. In addition, the infringing acts and practices of Defendants have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Textile is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Defendants are finally and permanently enjoined from further infringement.

153. Defendants have had actual knowledge of the 454 Patent at least as of the date when they were notified of the filing of this action. By the time of trial, Defendants will have known and intended (since receiving such notice) that their continued actions would infringe and actively induce the infringement of one or more claims of the 454 Patent.

154. In the post-suit period, Defendants have also indirectly and willfully infringed, and continue to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

155. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

156. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

157. In the pre-suit period, Comerica has indirectly infringed the 079 Patent and the 802 Patent by inducing others to directly infringe the 079 Patent and the 802 Patent. In the post-suit period, Defendants have indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Defendants have induced the end-users, Defendant's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

158. Defendants took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

159. Such steps by Defendants included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

160. Comerica has performed these steps, which constitute induced infringement, in the pre-suit period with the knowledge of the 079 Patent and the 802 Patent and with the knowledge that the induced acts constitute infringement. Defendants have performed these steps, which constitute induced infringement, in the post-suit period with the knowledge of the

079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts constitute infringement.

161. Defendants were and are aware that the normal and customary use of the Accused Instrumentality by Defendants' customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Defendants' inducement is ongoing.

162. Defendants direct or control the use of the Accused Instrumentality nationwide through their own websites, servers, and in their own branches, including in Texas and elsewhere in the United States, and expect and intend that the Accused Instrumentality will be so used.

163. Comerica took active steps, directly and/or through contractual relationships with others, in the pre-suit period with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes, for example, at least Claim 1 of the 079 Patent and Claim 1 of the 802 Patent. Defendants took active steps, directly and/or through contractual relationships with others, in the post-suit period with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

164. Comerica performed these steps, which constitute induced infringement, in the pre-suit period with the knowledge of the 079 Patent and the 802 Patent and with the knowledge that the induced acts would constitute infringement. Defendants performed these steps, which constitute induced infringement, in the post-suit period with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

165. Defendants' inducement is ongoing.

166. Defendants have had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

167. Defendants' customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

168. Defendants encouraged their customers' infringement.

169. Defendants' direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile' rights under the patents.

170. Textile has been damaged as a result of the infringing conduct by Defendants alleged above. Thus, Defendants are liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Defendants, and that the Court grant Textile the following relief:

a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Defendants and/or all others acting in concert therewith;

b. A permanent injunction enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by such entities;

c. Judgment that Defendants account for and pay to Textile all damages to and costs incurred by Textile because of Defendants' infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;

d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Defendants' infringing activities and other conduct complained of herein;

e. That this Court declare this an exceptional case and award Textile its reasonable attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 11, 2022

Respectfully submitted,

Matthew J. Antonelli
Texas Bar No. 24068432
matt@ahtlawfirm.com
Zachariah S. Harrington
Texas Bar No. 24057886
zac@ahtlawfirm.com
Larry D. Thompson, Jr.
Texas Bar No. 24051428
larry@ahtlawfirm.com
Christopher Ryan Pinckney
Texas Bar No. 24067819
ryan@ahtlawfirm.com
ANTONELLI, HARRINGTON
& THOMPSON LLP
4306 Yoakum Blvd., Ste. 450

Houston, TX 77006
(713) 581-3000

Stafford Davis
State Bar No. 24054605
sdavis@stafforddavisfirm.com
Catherine Bartles
Texas Bar No. 24104849
cbartles@stafforddavisfirm.com
THE STAFFORD DAVIS FIRM
815 South Broadway Avenue
Tyler, Texas 75701
(903) 593-7000
(903) 705-7369 fax

Attorneys for Textile Computer Systems, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on the 11th day of October 2022, a true and correct copy of the above and foregoing document was served on counsel for Comerica Bank via email.

Matthew J. Antonelli